TIA

Framework to Combat Fraud

Preventing and Responding to Fraud and Theft

TIA Framework to Combat Fraud

April 2024

Transportation Intermediaries Association
1900 Duke Street, Suite 300
Alexandria, VA 22314
Phone: (703) 299-5700
Fax: (703) 836-0123
www.tianet.org

TIA understands this document to be a working draft which may be updated from time to time.
TIA is interested in any and all constructive feedback and advice which could improve this framework.
Please email advocacy@tianet.org, and they will inform the committee of your concerns.

Chairman's Note

Every day we expose ourselves to many risks in our businesses. We are trusting people that in most cases we have never met to move products around the country that are worth exponentially more than the rates earned for moving those products. How we manage those risks improves our bottom lines and protects our customers.

This resource was originally compiled in 2014 to assist you and your teams with avoiding fraud in its many forms. Because the criminals are coming up with new methods every day, we offer this updated version to address additional forms of fraud (cybersecurity and internal theft) and to provide additional details to the types from the first edition.

The TIA also offers the TIA Watchdog, a web-based forum for the industry to report information on problems to each other. Together, these resources offer the opportunity to conduct your business in a manner that avoids these types of risks so that you can be more aggressive in other areas.

The TIA Fraud Task Force is comprised of a hand-selected group of people with unique experience in their area of expertise. We thank the members of the 2024 Task Force and those other TIA members who are and were integral in the development of this updated Framework.

The goal in business is to simplify logistics to promote capitalism as the greatest economic system. Our goal as a committee is that through these insights, you are able to prosper in your business endeavors without unnecessary risk.

Sincerely,

Dan O'Sullivan
Chairman, TIA Fraud Task Force

Disclaimer

The purpose of this Framework is to assist TIA members in developing and implementing their own policies and procedures to reduce potential for theft and/or fraud. The ideas, information, and suggestions in this document are only one set of tools for TIA members. It is the Committee's hope that this framework will encourage TIA members to take advantage of additional resources to reduce their exposure to the risk of loss, liability, and/or potential fraud. This framework is understood by TIA to be a "working draft" and evolving document.

The Framework is not designed, intended, or recommended to be a checklist or industry "standard." It is neither a characterization or summary of industry standards, nor a collection of "minimum thresholds" for motor carrier selection. All suggested tasks and acts may not be appropriate for every circumstance, and no single company or individual on the TIA Committee performs, recommends performing, or intends to perform most or all of the tasks or areas suggested for review.

Nothing in this Framework is intended nor should be used as legal advice or as a substitute for legal

advice which each member should obtain from qualified counsel familiar with the member's business and laws applicable to it. The Framework is not intended to define or prove compliance or non-compliance with any legal standard of care or diligence, and it should not be used or relied upon by anyone for any such purposes.

Table of Contents

SECTION 1: THE PROBLEM

I. Cargo theft and the rise of strategic cargo theft

According to CargoNet, cargo theft is up 600% from November 2022 to March 2023. Theft is at a 10-year high and strategic theft is primarily to blame. Criminals in the industry are being more selective in their targets and using sophisticated technology to carry out their schemes. The consequences of cargo theft reverberate throughout the industry as losses affect every part of a supply chain and ultimately raise the cost of goods to the consumer. Typically, the most commonly stolen goods are food and beverage, household goods, and electronics. California, Texas, Illinois, and Florida routinely top the list for states with the most incidents of theft followed by Georgia, Tennessee, Pennsylvania, Arizona, and Ontario. To be more specific, San Bernardino, CA, Los Angeles, CA, Dallas, TX, Cook County, IL, and Miami-Dade, FL, top the charts for most thefts in 2024.

In September 2022, strategic cargo thefts began in earnest. Strategic theft uses deceptive means, such as stolen identities, rather than engaging in the more traditional methods of direct theft, where freight is targeted at truck stops, drop lots, etc. The industry is seeing more cybercriminals conducting strategic cargo theft or fictitious pickup schemes online by impersonating legitimate parties through forgery and identity fraud. The criminals may pose as a legitimate motor carrier (MC) or freight broker to get a load, then turn around and put it back on a load board to get a legitimate driver to carry it somewhere. Their goal is to pass a load through multiple drivers and warehouses to essentially launder the shipment. Once an outlier, the imposter shipper scam is becoming much more common. Criminals are now frequently posing as the shipper, using shipment data gathered by impersonating a broker or carrier, then pretending to be the shipper. Once they convince someone to pick up the shipment, they either route it to a new destination or run it through a series of warehouses.

Decreased freight rates are also a big contributor to the rise in strategic cargo thefts. When rates are low and cargo harder to find, carriers are less likely to thoroughly scrutinize potential loads. This is especially true when a criminal posts a fraudulent load with a higher per-mile rate. When the unsuspecting carrier takes the load from the fraudulent broker, it is picked up with the correct pick-up number and destination information, which leads the shipper to load them with no hesitation. Shortly after the carrier picks up the cargo, they are contacted by the fake broker and are offered Zelle, PayPal, or another form of quick payment, to take the load to a nearby cross dock facility or warehouse with the fake broker telling them that their customer needs to change the address last minute. The criminals re-route drivers to these warehouses and cross-dock facilities where warehouse receipts are created, new Bills of Lading (BOLs) are generated and usually the load goes right back out after it is delivered to another unsuspecting carrier. If they get stopped by authorities or DOT, they have a legitimate BOL. This makes the shipment almost impossible to trace, and usually the original broker gets stuck with the stolen load cargo claim.

Cargo theft costs small businesses, who already work on small profit margins, millions of dollars each year in stolen merchandise. The transportation sector must develop adaptable tools to meet a constantly evolving threat. Advancements made in technology have added several weapons to the industry arsenal to combat criminal conduct. The TIA Fraud Task Force intends to expand the dialogue on this issue, so that industry members can identify, discuss, and perfect new policies to mitigate their exposure to theft and fraud.

Data provided by the team at Verisk, for 2020-2022 illustrates trends in cargo theft during those three years.

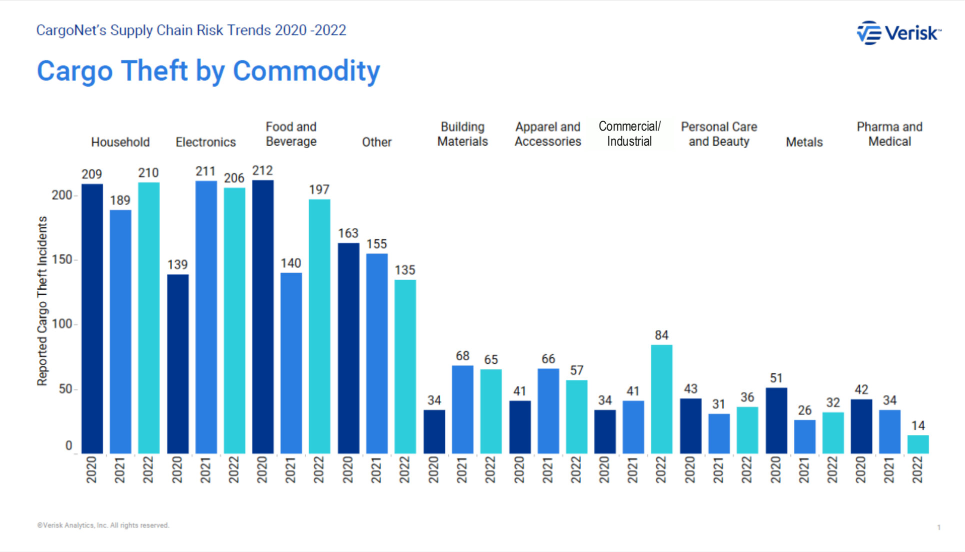


Figure 1: Theft by Commodity 2020-2022, Data Courtesy of Verisk

The most common locations where thefts occurred were warehouses/distribution centers, parking lots, truck stops, and from secured yards owned by carriers.

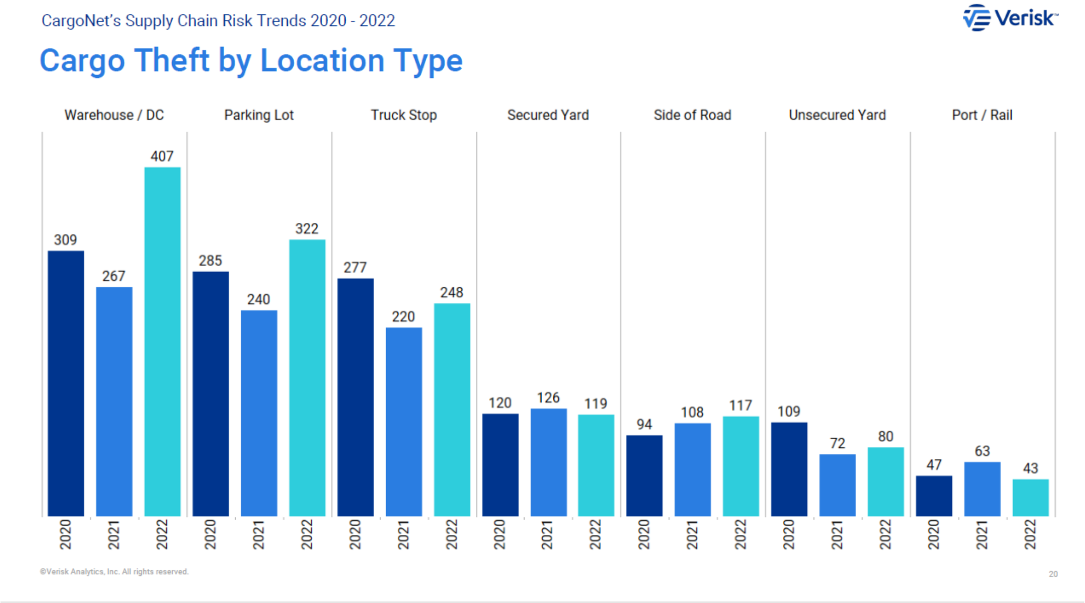


Figure 2: Theft by Location 2020-2022, Data Courtesy of Verisk

Finally, data provided by Verisk shows that cargo thefts occur more often between Monday and Friday. In the three years of data shown below, a maximum of 22% of thefts are reported on Saturday or Sunday; 78% of thefts are reported during the week.

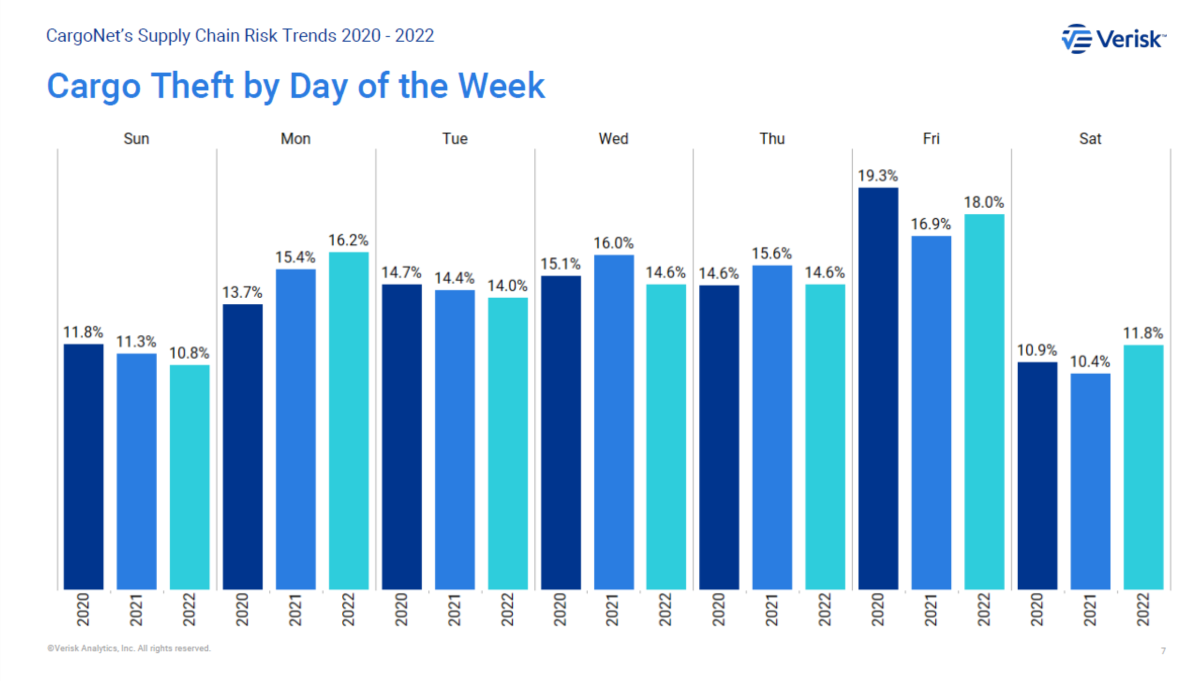


Figure 3: Theft by Day of Week 2020-2022, Data Courtesy of Verisk

A. Strategic Cargo Theft Case Study #1

One broker experienced vindictive behavior by a carrier they had used for several years. The carrier experienced a delay running a load for the broker in 2018 which resulted in a charged late fee. Two years later, the carrier picked up a load of home appliances for the same company. The broker experienced unsatisfactory communication from the carrier and relied on Macropoint to provide the majority of the transportation updates. Multiple Macropoint pings revealed the carrier had not been moving and the broker called the carrier to find out why.

The carrier revealed that they had plotted to steal this load as vengeance for the late fee from 2018 and that they would hold the load “hostage” until their demands were met. The broker agreed to meet the carrier’s demands, and the carrier provided a new phone number to Macropoint. The new Macropoint ping revealed the load was several states away and on route to a cross-country destination. At this point in time, the cargo was one day late for delivery. According to the broker, the new phone number pinged Macropoint multiple times from the same location of the cargo. The load was no longer moving.

The broker discovered that this load was being double brokered by the carrier and that the updated phone number provided was for a partnering brokerage several states away. Utilizing the new phone number provided by the carrier showed false Macropoint updates and the broker again could not find the load. The carrier demanded additional freight be prepaid in order to reveal the location of the cargo. Per the broker, the carrier had no intentions of delivering the cargo as originally contracted and demanded full freight payment for two loads, one of which they didn't deliver, and reimbursement for the 2018 late fee. Once those demands were met, the carrier advised that the cargo was in a warehouse near the shipper and provided the accurate address. Unfortunately, the cargo had been damaged during this transport. In the end, the customer took the load back from the broker and delivered the cargo themselves.

B. Strategic Cargo Theft Case Study #2

On March 28, 2019, the broker booked the carrier on a load-out trailer moving cargo from Saginaw, TX, to Laredo, TX. Per the rate confirmation, the trailer was to be picked up by the carrier on March 28 and delivered on April 4. The carrier told the broker that the trailer was delivered on April 5, 2019. When informed by the receiver that the trailer never arrived, the broker was told by the carrier that the trailer would instead arrive on April 11, then April 12, and then again on April 16, when the carrier called the broker to say that they were finally checked in and waiting to unload. On April 23, the customer contacted the broker, saying that this trailer had not yet arrived at the destination in Laredo, TX. From this point on, the carrier stopped responding to calls and emails.

After further investigation into the carrier in possession of the customer's trailer, it was discovered that the insurance policy for the carrier was cancelled in April 2019. A stolen trailer report was filed with CargoNet and with Saginaw, TX, Police Department for a missing/stolen 2020 Hyundai 53' Dry Van Swing Door Trailer. Around the same time, the broker sent a different driver to the address on file for the carrier to see if contact could be made with someone in person. The broker was informed by this driver that the physical address on file for the carrier was not their business, but was actually a bread shop. The only contact the broker made with the carrier in May was a phone call with one employee; he claimed he did not speak English and abruptly hung up.

During the investigation with Saginaw PD and CargoNet, it was determined that the carrier was a fraudulent company. There were four other companies associated with the carrier, linking multiple names and phone numbers to the same address as the bread shop. All four companies also had FreightGuard reports in Carrier411 for stolen trailers, with one claiming "TRAILERS ARE NOW 3 WEEKS LATE AND HAVE GONE INTO SEVERAL OTHER STATES. WE HAVE HAD LITTLE TO NO COMMUNICATION FROM THEM. FURTHERMORE, OUR CUSTOMER NOTIFIED US THAT [CARRIER] HAS STOLEN EQUIPMENT FROM THEM IN THE PAST AND WERE SELLING PRODUCT OUT OF THE TRAILERS AND ADVERTISING ON FACEBOOK."

To date, the trailer has not been recovered, and the files are still open with CargoNet and Saginaw PD.

C. Strategic Cargo Theft Case Study #3

On September 19, 2022, a broker received a phone call from a posted load and booked a shipment with non-Safer verified contact using a legitimate MC number. The broker did not book with a verified contact and emailed the rate confirmation to a scammer pretending to be an MC at dispatch1234@gmail.com (not the actual email address but very close to the scammer's email). The shipment contained 24 pallets of solar panels with an approximate weight of 39,600 lbs. The load was picked up in Gardena, CA, on the afternoon of September 19 and was scheduled to be delivered to Hammond, IN, the following day.

On September 26, the owner of the cargo notified the broker that the load had not yet arrived. When the broker contacted the carrier, he found out that the people who booked the shipment (known as Simon and Mario), were not actual employees for the carrier. The carrier had been a victim of identity theft and denied having picked up this shipment. Simon had played the role of dispatcher while Mario played the role of the driver.

After investigating further, the broker discovered that a different MC was the actual carrier that picked up the freight. When speaking with the other MC, they said they were given the load by another broker to deliver to Sacramento. The rate confirmation received from the fake broker had them deliver to Sacramento, CA. The MC that was hired by the fraudulent broker and who picked up the cargo also mentioned to the broker that the address for delivery was changed to an address in McClellan, CA. The carrier did not know the name of the building or the contact information for the people that unloaded them. The broker had to file this theft with their contingent cargo insurer after filing the loss with the carrier who had their ID stolen.

D. Strategic Cargo Theft Case Study #4

The broker booked what he believed was a legitimate MC on April 4 to transport a load of JVS televisions from City of Industry, CA, to Portage, IN. Following SOP, the broker arranged the shipment with the SAFER registered contact information listed. Shortly after the load was booked, the shipper pushed the load pickup date from April 4 to April 6. The broker notified JVS of the change and they had no issue. The next day, April 5, the shipper notified the broker that the load had already been picked up. The SAFER contact said the shipper loaded his driver the day before and stopped responding to all emails after that. The load was never delivered. When the broker requested pictures from the shipper of the truck picking up, they sent them pictures which appeared to be a different carrier. When the broker confronted the other carrier about their truck being at the shipper, they informed the broker that it was not their truck, and an ex-dispatcher they used to use had someone re-placard a random truck for this pickup. The broker also noticed that the fraudulent carrier had listed their contact information in the other carrier's RMIS profile, and the same dispatcher was accepting loads under both MCs. The broker had to file this theft with their contingent cargo insurer after filing the loss with the carrier.

E. Strategic Cargo Theft Case Study #5

An MC was set up with the broker in April 2023, and they delivered two loads successfully without incident. The following month, over the course of a few weeks, the carrier booked multiple loads of electronics on the broker's app. They always picked up on time but there were delivery delays on most shipments. The carrier would eventually deliver and submit what the broker thought was a clean Proof of Delivery (POD). However, it turned out that the carrier double brokered the shipment and provided a fraudulent POD to obtain payment. The customer reported there were shortages on multiple deliveries and that the POD submitted by the brokers carrier was falsified to hide the pilferages. The carrier used a fake Sam's Club DC stamp and submitted fake PODs with only a portion of the loads delivered. The carrier repeated the same scam on six different loads, stealing more than $200,000 worth of cargo. The broker had to file this theft with their contingent cargo insurer after filing the loss with the carrier.

F. Strategic Cargo Theft Case Study #6

The broker booked with an MC for a liquor shipment originating in Kentucky and destined for Las Vegas. The driver began tracking electronically but shut off tracking early in the trip. Driver and dispatcher communication was spotty at best. Eventually the driver claimed to have broken down in Salt Lake City, but refused to provide a repair shop address, claiming that he was afraid the broker would steal his trailer. He did this to buy time for what he was actually doing which was to move the load to Mexico for sale. Eventually the driver furnished a fake shop invoice and attempted to solicit a Comchek from the broker. This was an attempt to scam even more money from the broker. The dispatcher-owner claimed that the driver had gone rogue and that he had just signed on with the company a couple of weeks prior; that the driver convinced the dispatcher to let him book his own loads so he could shop for liquor shipments to steal using someone else's MC. The CDL provided by the dispatcher-owner was a fake. The other scenario is that the dispatcher-owner was in on the scam and was trying to keep its TIA Watchdog record clean by claiming to be a victim. The carrier's insurance has an exclusion for willful misconduct of a driver and the claim fell on the broker's contingent cargo insurer to respond to the loss.

G. Strategic Cargo Theft Case Study #7

The broker booked an MC that had been in their network for years with a 20-year-old MC number and a long history of loads with the broker. When a transported load never showed up for delivery, the broker learned that the previous owner sold the business to a fraudulent entity and was using their good name and legacy MC number to infiltrate broker networks to steal freight.

MEMBER-SUGGESTED CHECKLIST FOR PREVENTION

1. Verify that who you are talking to is a legitimate contact for the MC you are doing business with. If the carrier has had contact changes within the last 60 days, consider it a red flag and re-verify with a known point of contact. Usually, the carrier whose ID has been stolen has no idea.
2. Always give your shipper the MC number of whoever is supposed to pick up and have them take photos of the drivers CDL, truck, and trailer that show their MC and DOT number and license plate. Have the shipper turn away any carrier not hired by you.
3. Use extreme caution when booking targeted commodity loads such as solar panels, appliances, electronics, tires, food and beverage, and non-ferrous metal loads.
4. Always implement technological tools to help track your cargo such as disposable GPS tracking within your pallets. Shippers can also establish Geo Fences along major highway systems that alert shippers if a driver diverts from an expected route. Track and Trace networks also diminish the odds of a carrier going missing due to compliance requirements with their programs.
5. Do not rely on one technological tool; diversifying your technology services improves your odds of preventing theft. Some services can be manipulated or turned off. Note: if you hope to depend on ELD tracking to find your loads, a warrant issued to the manufacturer may be required to obtain that tracking information, and this can be a lengthy process.
6. Properly vet your carriers and verify that the assets they are using belong to them. Third-party services also offer fraud and alert searches relating to the MC with which they are registered. Consider integrating an API tool that automates this process and partnering with a reputable Track and Trace service.
7. Read your insurance policy! Insurance coverage depends on what type of coverage you have. If the carrier was fraudulent from the start, the insurance company may have no responsibility to honor any claim. Know your insurance and make sure it actually covers what you think it does. Consider discussing a shipper interest "All Risk" program with your insurer to cover known high-value commodities. Various insurance and broker liability policies and programs exist. It is important to understand the insurance coverage you are paying for.
8. Speed is of the essence when dealing with theft. Treat every theft as if you have only 48 hours to recover stolen cargo. Report thefts immediately to improve your chances of recovery. After the first 48 hours it is generally acknowledged that the chances of recovery drop by almost 50%.

9. Make sure the carrier's paperwork is actually read and verified. Clearly communicate your contract terms to carriers to prevent unforeseen issues.

10. Gather as much information as possible that might be useful to authorities in the event of an investigation (see Addendum 1, Sample Incident Intake Form). Valuable information includes a picture of the driver's license, any video of individuals loading the truck, the name of the carrier from the side of the truck, and supply invoices proving the value of the product and losses incurred. Be prepared to share this information with anyone who will listen. Video surveillance is cheap and high quality. Consider investing in surveillance video that is positioned to capture the license plates of any vehicles (trucks or trailers), as well as vital information on the trucks or trailers, rear of trailers, and the interior of trailers.

11. Request that the carrier file a claim with their motor truck cargo carrier. Some contingent cargo policies require this for your coverage to be triggered. If a carrier is being uncooperative during this process, feel free to contact their insurance agent to expedite the filing process or send a demand letter to the carrier and copy its insurer on the demand. If the demand alleges something that would be covered, this may pull the insurer in.

12. Contact/Notify: Shippers, produce markets affected, industry trade guides, regional cargo theft recovery groups, process agents, insurance companies, load boards, and credit reporting agencies.

II. Financial Theft

Financial theft is a method of fraud that frequently offers a low-risk, high-reward proposition for potential criminals. Methods of financial theft are varied, but strategies which have been identified by transportation experts include: Comcheck or T-Chek cash-advance schemes, fraudulent or altered paperwork, extorting receivers by holding loads hostage, double brokering, check fraud and false factoring or invoicing.

A. Financial Theft Case Study #1

The broker posted a load on the load boards and was contacted by someone impersonating a legitimate carrier. When dispatched, the driver then created a falsified BOL using information provided by the shipper. When the broker requested a copy of the pickup BOL, the fake BOL was submitted, and an advance was given to the impostor. In most cases when this happens, the load was never picked up from the shipper.

B. Financial Theft Case Study #2

The broker posted a hot load on a load board. A legitimate carrier called and booked the load and was overly eager to take the load. The driver picked up the load and on the way to the consignee the truck broke down three times. The final breakdown happened just as the carrier left the repair shop. The DOT placed the carrier out of service. The truck was left in front of the repair shop. The carrier's owner did not have the funds to pay for the final repairs and the repair shop would not release the cargo until the repairs were paid for. The towing company also needed to be paid for delivering the cargo to its final destination.

The carrier was uncooperative through the whole transaction. The repair bill was in excess of $3,700.00 and had to be paid by the broker.

C. Financial Theft Case Study #3

The broker mailed a check to the carrier. The check was intercepted by someone who copied the check and, using modern scanning and printing technology, reproduced multiple checks with a "legitimate" signature, format, and amounts. The checks used numbers that were current to the broker's account. These checks were then cashed (usually in batches) and by the time the broker realized the fraud, the perpetrators had disappeared with the money. Depending on the broker's agreement with their bank, they may have been liable for the full amount. This type of theft happens most often around the holidays when a broker's staff may be on vacation or stretched thin.

D. Financial Theft Case Study #4

The broker tendered multiple loads to a small or midsize carrier. That carrier then took the loads they accepted and brokered them out to other carriers (referred to as double-brokering), offering to pay more money than they contracted for. The initial carrier made check calls back to the broker and obtained a copy of the BOL and POD and forwarded their invoice for payment. Months later, the broker was advised that their carrier double-brokered the freight and did not pay the actual carrier for the load. The original carrier was no longer in business and collection agencies contacted the broker's customer for payment.

MEMBER-SUGGESTED CHECKLIST FOR PREVENTION

1. Many brokers have stopped giving fuel advances and created additional measures to limit advances.
2. Make sure any change to carrier information is verified. Contact numbers for carriers directly to ensure a connection between carriers and drivers.
3. Brokers should contact shippers directly to request they write down the name of the carrier who picked up the load (not all shippers will agree to this).
4. Brokers should contact the shipper again to verify that the load was picked up.
5. Ensure new carrier legitimacy by double-checking insurance and verifying their authority for pickup. (ex: SaferSys or to verify Texas Intrastate DOT Numbers).
6. Use TIA Watchdog and other technology solutions when working with new carriers to see if they have any record of recent potentially fraudulent activity.
7. Periodically check load boards to see if someone is posting loads that look like yours and investigate to make sure yours are not being double-brokered.
8. Enroll in your bank's positive-pay system to avoid fraudulent checks being cashed and limit liability.
9. Verify carrier's financial stability by researching their credit history using a credit reporting service.

III. Identity Theft

In this world of fewer face-to-face interactions, it is often difficult to verify the identity and credentials of the people with whom one does business. The reputations and financial well-being of brokers, reliable shippers and carriers, employees, and customers are at stake in any identity theft situation. Due to these risks, brokers must be diligent about safeguarding their own information and verifying facts with shippers and carriers.

A. Identity Theft Case Study #1:

The brokerage company began receiving invoices from carriers for loads that were not displayed in the brokers' system. Some carriers have carrier load confirmations showing the broker company name, complete with an address and phone number similar to the broker's. However, those load confirmations were quickly identified by the broker as fraudulent.

Aware that the company identity had been stolen, the broker immediately contacted TIA and the load boards to report the theft. However, the broker continued to receive fraudulent carrier load confirmations. Eventually, the broker contacted a credit services company which "flagged" the account without disrupting the broker company's credit score. This flagging led to freight factors contacting the broker to verify their client invoices were valid (a burden), but it did prevent carriers from taking loads from the party issuing the fraudulent invoices. As a result, the thief ceased using the company's name on the false invoices.

B. Identity Theft Case Study #2:

A new customer called with three loads of products that needed to be moved. Credit was checked, customer credentials (address/phone) were verified, and a contract was executed. The new customer contact stated they worked from home, so an alternate telephone number was provided for load updates. The loads were picked up and delivered without issue. The loads were processed normally and the carriers were paid. When payment was not been received after 30 days, a collection call was made to the customer's company where it was revealed that the customer had never heard of the broker and never authorized the loads to be transported. A call to the customer contact "home" phone shows the number was disconnected. The consignee was a warehouse, and the product had disappeared.

MEMBER-SUGGESTED CHECKLIST FOR PREVENTION

1. Verify, verify, verify! Do your best to ensure that you are dealing with a legitimate carrier or customer. If something doesn't match (like a phone number), check it out. Watch for imposter web addresses, e.g., the carrier's name with an extra letter or something other than a .com.
2. If possible, have the shipper verify the name on the door of the carrier picking up your load; even better, have them take a picture of the driver's license.
3. Create special pickup numbers only shared with the shipper and the driver you dispatch. This will prevent another driver overhearing the dispatch information from picking up the load before your driver arrives.
4. Do not include your license or bond copy in a new carrier packet or on your website. Make the information available to any carrier who requests it upon verification that the requesting party is legitimate.
5. Even without securing all information on a company, a perpetrator of identity theft can still set up with new carriers if those carriers do not verify with whom they are doing business.
6. Ensure that carriers and shippers mind their records and check for discrepancies such as the contact information in load confirmations.
7. Report any theft to TIA, load boards, Department of Transportation Office of the Inspector General, carrier monitoring services, credit reporting agencies, and anyone else who can help pass along the information. More harm can be done to your company's reputation by someone who steals your identity

than by acknowledging that your identity has been stolen. Carriers will appreciate your efforts to try to protect them.

Criminals are getting smarter and bolder, unfortunately, so that means we have to as well.

IV. Internal Theft

One of the biggest betrayals a business owner can experience is when someone who is trusted and paid to do a job uses that position to harm the company.

A. Internal Theft Case Study #1:

A small brokerage had limited administrative staff. One person made the deposit, entered the payments into the TMS, and reconciled the bank statement every month. When that employee took a vacation, it was discovered that some checks had not been deposited into the company account but had instead been deposited into the employee's account. A bogus journal entry was created to cover up the theft. The crime was discovered by an alert customer who noticed that the check endorsement was different and called the brokerage owner.

The employee was terminated and charged. Afterward, the brokerage owner divided the cash duties, so the same person did not handle the entire cash transaction. If someone created the deposit, someone else entered the details into the TMS and each employee signed off on a cash-flow report when they balanced. The owner took on the job of reconciling the bank statement each month.

B. Internal Theft Case Study #2:

An agent's contract was terminated for non-performance. A few months later, the brokerage received several past-due invoices from an LTL broker for loads that did not match up with loads in the brokerage's TMS.

After calling the LTL broker, the brokerage owner learned that the terminated agent had set up an account for the brokerage in the LTL broker's TMS (the agent was a former agent for the LTL broker as well) and had changed the billing address on the brokerage account and set up the account so that the brokerage would not receive the invoices. The agent had the customers on these loads pay him directly. The LTL broker discovered the scheme during its collection process but insisted that the brokerage owed payment to them and tried to sue for non-payment. The brokerage prevailed in court but sustained legal fees to defend the suit. The brokerage attempted to file charges against the terminated agent but ran into jurisdictional issues as well as an address and phone number that was no longer valid.

MEMBER-SUGGESTED CHECKLIST FOR PREVENTION

1. Run background checks on new employees or agents. Verify employee references, if provided.
2. Do not allow one person to handle the entire cash transaction process. If hiring additional staff is not feasible, do at least part of the process yourself.
3. Periodically, switch jobs around so the same person doesn't do the same task all the time. Not only will this cross-training help your office to be more efficient, but it will also make it harder for employees to commit internal theft.
4. Limit the available information on your company to agents. Do not provide them with copies of your MC and make sure this vital information is not part of your new customer or carrier packets.

V. Data / Information Theft

The importance and value of a company's information and data is constantly increasing, as is the need to protect it. Cybercrime refers to a broad array of criminal activities performed via computers, including the theft of a company's employee, customer, carrier, and other stakeholder information. There are many methods a bad actor may use to access valuable company data, including but not limited to black hat hacking, social engineering (e.g., phishing email), and installing ransomware.

A. Data / Information Theft Case Study #1:

An employee at a brokerage received an email with access to an internet-based shared file. The employee clicked on the link, inadvertently installing a ransomware virus on their computer, which spread to the entire network. The ransomware shut down critical systems, blocking access to information critical to operations. An electronic ransom note demanded bitcoin payment to unlock systems and data.

B. Data / Information Theft Case Study #2:

A group of foreign cybercriminals scanned the internet-facing network of a brokerage, finding a common hole left open in the firewall. These hackers penetrated the firewall and accessed the company's central store of usernames and passwords. This information, along with employee data including social security numbers, were sold on the dark web. The company's employees learned of their stolen identities in the following days and weeks.

C. Data / Information Theft Case Study #3:

A bad actor working on behalf of a competitor drove into the parking lot and parked next to the building and, using a computer, logged onto an under-secured Wi-Fi network. From their car, this cybercriminal accessed network resources, copying customer and carrier contacts, along with pricing models and financial records.

D. Data /Information Theft Case Study # 4

A fraudulent entity posing as a motor carrier sent a phishing email to a broker in response to a load posting. The scammer said "I am interested in this load, but I am concerned about the negative review someone wrote about you on the loadboard. See this link." The broker clicked on the link which lead to a fake loadboard landing page designed to look exactly like the real loadboard. The broker signed in and was redirected to the real loadboard. In the meantime, the scammer had captured the login credentials of the broker on their server. The scammer then used those credentials to post double-brokered loads using the broker's name. This is particularly common with power-only loads from other load boards such as Amazon Relay. Eventually the carriers and their factoring companies began to inquire with the broker about payment status, and although the broker had no liability to pay shipments that were not theirs to begin with, the event had a negative impact on the broker's reputation and creditworthiness with factoring companies and carriers. Victim-carriers may attempt to file on the broker's bond, a claim that has an easy defense, but it shows up on the broker's record nonetheless when bond underwriters renew the policy.

MEMBER-SUGGESTED CHECKLIST FOR PREVENTION

1. Ensure firewalls and Wi-Fi networks are secure and tested periodically. Cybersecurity companies are available to do this if in-house staff is not adequate.
2. Set up a culture of information protectionism and perform ongoing end-user information security education.
3. Test company employees' ability to identify suspicious emails, phone calls, and behavior. This should include, at a minimum, email phish testing.
4. Create and implement an acceptable use policy, which should include password, mobile access, and email policies, along with simple data classification.
5. Implement secure (off-line) data backups with enough frequency to enable restoration of data in case of a virus or ransom-ware attack. Multiple sets of backup data will increase data security.
6. Test restoration and recovery of systems and data at least once per year to account for changes in software, hardware, or personnel.
7. Create a written Emergency Response Plan which includes recovery process and communication to stakeholders.

SECTION 2: THE NUTS & BOLTS

PREVENTION

I. Fraud & Theft Prevention Best Practices

There is an old adage that says, "An ounce of prevention is worth a pound of cure." That is true in today's transportation industry. The steps you take in selecting carriers is not only important in providing service to your customer but is also important in preventing issues and potential liability that could result in financial loss to you (the broker), your customers, and others. This section will help you to understand the importance of having preventive measures in place and help you to identify steps to help mitigate risks.

MANAGE YOUR OWN RISK & EXPOSURE

There are many steps a broker can take to protect their company before they start brokering loads and vetting carriers. Below are a few high-level actions brokers can take to manage their own risks and exposures.

1. Protect your company's information. Do not put your authority or bond documents on your website. Only send copies of your authority and bond upon request to verified recipients.
2. Use contracts. A signed contract provides a written agreement between all parties that clarifies liability and helps provide recourse in courts. TIA strongly encourages members to use TIA's model contracts as a starting point for their contracts (www.tianet.org).
3. Procure proper insurance against certain risks that are inherent to your existing business and plans for future growth. In evaluating risks and insurance, consider whether the insurance would offer added protection from fraud and fraudulently induced liabilities that may arise within your business and its relationship with shippers, carriers, and others.
4. Create a carrier vetting policy and protocol. Implementing procedures for carrier selection is an important step to reducing fraud. Strong carrier selection allows you to vet aspects of a business that are more susceptible to fraud. See the next section for a detailed guide on how to do so.
5. Work with organizations that supply cargo theft trends and data analytics about cargo theft and fraud. Data is power and, by using cargo theft analytics, one can better identify risks within their own scope of the supply chain. The information can be used to perform carrier history checks. Be selective in arranging carriers, particularly when it comes to safety and areas of greater risk for theft and fraud. Provide motor carriers with appropriate information at the appropriate times to avoid being a victim.

II. Thoroughly Vet & Maintain Your Carrier Network

A. Develop a Detailed Carrier Selection Procedure and Protocol

You can use TIA's Carrier Selection Framework as a reference for some ideas to incorporate into your carrier vetting process. While not verbatim, the section below provides a summary and overview of TIA's Carrier Selection Framework. Some additional or different considerations have been added.

B. Develop a Process for Collecting & Verifying FMCSA Carrier Information

Collect information on operating authority and insurance directly from the carrier. Then use a combination of the sources below to verify the accuracy of the information provided by the carrier:

- Internet searches
- FMCSA Website for Licensing & Insurance
- FMCSA Safety & Fitness Electronic Record System (www.SaferSys.org)
- Your own company database. When you contact a carrier you would like to engage, be sure that you are using verified contacts for the carrier. You can typically verify via FMCSA websites or through your carrier on-boarding vendor.
- Re-verify carrier information on a recurring basis (i.e,. semi-annually). Force re-verification for any contact information changes with FMCSA within the last 60 days.
- Leverage third-party carrier monitoring services that provide motor carrier operating authority, safety, and insurance information. If doing so, understand how often the data is updated (the more frequent, the better).
- Validate the address, phone number, and email to ensure the information provided is unique and does not match another DOT or MC. If the information provided matches another MC or DOT number, it could be a sign the carrier has previously existed under another MC. Businesses can use different carrier monitoring sites to help identify chameleon carriers or set up their own monitoring tool leveraging the publicly available FMCSA data.

Be aware of inconsistencies. If there are differences between the information provided by the carrier and information that is publicly available, request clarification from the carrier or agents who provided the information.

C. Verify Paperwork Provided

To reduce fraud in your network, properly vetting paperwork submitted by the carrier is an important step. Verification can be a manual process, or you can leverage technology to do most of the work.

1) Operating Authority

- Verify the authority granted by FMCSA.
- Common carriers are granted a certificate, while contract carriers are granted a permit, and brokers are granted a license. If the letter says the carrier is a common carrier, but the authority is shown as a permit, it may be fraudulent.
- Verify that the MC number and information matches the FMCSA licensing website.
  - Official agency-issued letters are HIGHLY standardized. Review the letter for unusual fonts and obvious spelling or grammar errors.
  - Review the carrier history on FMCSA's website for consistent patterns of Out of Service records or inactive authority.
  - Financially unstable carriers may show multiple "involuntary revocations" and authority reinstatements due to lapses in insurance coverage. Consider whether to accept "reinstatement"

authorities, unless the carrier can produce the original. (If a carrier went to work under someone else's authority or suspended operations for a period of time before reinstatement, the original may no longer be available. Reinstatement permits from FMCSA are completely valid.)

  - Verify with FMCSA that the carrier has a BOC-3 filing. Carriers are required to file for a BOC-3 agent in any state in which they operate.

2) Insurance Documents

- Check the length of time that the carrier has had authority and insurance, and verify that their insurance will be effective for the duration of the load that the carrier has been contracted to haul.
- Do not contact the insurance agent using the phone number provided by the carrier. Independently verify the insurance contact, then contact the insurance agent directly for copies of carrier insurance certificates. Scrutinize the certificates of insurance (examples of false certificates available in Section X.)
- Verify phone numbers and addresses. Make sure the carrier's name matches the FMCSA licensing website.
- Verify that the insurance company name, policy number, and effective dates match the FMCSA licensing website.
- Look for unusual fonts, or obvious spelling or grammar errors. If insurance certificates are unavailable from the insurer, verify carrier contact information on insurance as provided by carrier, and cross-reference it with information on file from FMCSA.
- If insurance certificates are unavailable from the motor carrier's insurance agent, verify the motor carrier contact information on the Certificate of Insurance as provided by carrier, and cross-reference with information on file from FMCSA.
- If auto liability insurance is a "Scheduled Auto" policy, request a list of insured equipment from the insurance agent. Then request a copy of the cab card from the driver to verify that the vehicle is on the list.
- If a small carrier (less than 50 trucks) carries auto liability insurance with a "Risk Retention" company (except OOIDA who is set up to work with small carriers), check the underwriting policies for the group. Typically, risk retention groups have very high deductibles and are geared more for medium (50+ trucks) sized carriers.

3) Carrier Safety Rating (United States)

- Verify the carrier's safety rating at www.safersys.org, "Company Snapshot."
- DO NOT knowingly use carriers with "Unsatisfactory" safety ratings.
- Some brokers choose not to use "Conditional" rated carriers. For brokers that may consider using carriers with this rating, additional diligence should be performed to assess if the carrier has appropriately addressed the underlying issues to the broker's satisfaction. Call the carrier's management and ask:
  - When the "Conditional" rating was received.
  - What reasons the carrier was given for the rating.
  - What has been done to correct the alleged infractions.
  - Whether a compliance review has been requested.

- Whether the carrier is taking additional steps to improve the rating.
- Request copies of any correspondence between the carrier and FMCSA regarding a "Conditional" safety rating and/or a compliance review.

- A large portion of carriers are "Unrated" by the FMCSA, currently around 92%. This is common since not all carriers receive audits that lead to Safety Ratings.

4) Carrier Safety Rating (Canada)

- If applicable to the geographical scope of your operation (you contract with Canadian carriers), Canadian carriers should meet your US standards as well as the Canadian safety standards you have deemed fit for your operation.
- Canadian carriers can be registered through the DOT, and you can leverage the same systems for verifying US carriers as you can for Canadian carrier performance in the United States.
- Leverage province-specific sites for their performance and safety information in Canada.
- Verify the carrier has not been deemed unfit to operate by the safety fitness determination procedures of an authorized agency of Canadian Federal, Provincial, or Territorial government.
- Canada's equivalent safety fitness determination may be used to determine whether a Canadian MC is safe to operate in international and interstate commerce.
- Canadian MC safety fitness determinations can be verified by navigating through www.safersys.org, or directly through the specific Canadian province website.

5) Additional Items To Verify

- Verify a carrier's Federal Employers Identification Number (FEIN or EIN) from the W-9 they file with the IRS (use www.irs.gov/taxpros/index.html, then click on e-services).
- In the event of a business name or ownership question, request to view the Secretary of State corporate or LLC filings, and verify that the information matches what is on file with the State.
- Contact the carrier's business, customer, and bank references.
- Verify the credit score or credit rating of the carrier.
- If the length of time a carrier has been in business is important to you, and the carrier is newly opened, you can:
    - Check the principal's credit history.
    - Verify with FMCSA that the carrier has passed its New Entrant Safety Audit.
    - Request a copy of the results of the FMCSA New Entrant Safety Audit.
- Even if a carrier is legitimate, limit the number of loads that a new carrier is allowed to book. It is important to build a relationship and understand carrier strengths and capacity.
- When reviewing carrier documentation, in addition to basic evidence, such as obviously forged documents or falsified contacts, also watch out for the following red flags:

  - Look for strange gaps in the carrier's authority history and investigate discrepancies.
    - For example, the authority of a carrier had been revoked for 19 years, then suddenly was reactivated in a different state hundreds of miles away. Such a circumstance occurs infrequently, and merits closer inspection. It should be noted that some carriers obtain old authority numbers (possibly through acquisition or other means) simply because some brokers refuse to work with new carriers.
    - Consider the number of trucks the person is telling you the carrier operates; for example, A carrier claims to have 1,000 trucks for a 2-month-old MC number.
- As mentioned above, when validating paperwork, it is important to verify that a carrier is not a chameleon carrier or an old carrier trying to come back into your network (meaning the carrier operated under one MC and then started up using another MC number). While there can be valid reasons for a carrier to do this, it is important to verify the safety scores and ratings of the carrier under the old MC. If the older MC does not meet the standards laid out in your carrier selection framework, you may not want to use the carrier. A chameleon carrier may be identified by a combination of the following:
  - Shares the same or similar business address.
  - Same phone number.
  - Same owner/contact and email address.
  - Similar VIN numbers for trucks used in the business.

6) Utilize TIA Watchdog in Your Carrier Selection Process

- Check TIA Watchdog for any complaints or warnings about the carrier.
- When onboarding, check the MC or DOT number in TIA Watchdog. If the results come back, review the comments by both the broker and the carrier.
- Remove carriers from your network who have flags or comments that do not align with your selection framework.
- Check TIA often. Even if a carrier has been in your network for some time, do frequent checks to make sure new flags have not surfaced.
- Contribute to TIA Watchdog by reporting carriers who engage in activities that warrant a flag in TIA Watchdog.

7) Collect Driver Information

For liability reasons, a broker should not exercise any control over an MC and/or a driver. However, an important part of fraud and theft prevention is obtaining information on the driver and vehicle used by the MC, and sharing information with the shipper, such as:

- Obtain a copy of the driver's license (if possible).
- If possible, obtain a clean electronic thumbprint from the driver.
- Request a driver to provide copies of his CDL and tractor/trailer registrations. This enables identity verification and ensures that the equipment carrying the load is insured.

- Request contact information for the driver or dispatcher including phone number and email. This provides the opportunity to directly reach out and create a written history of the relationship.

**Collecting personal information is important in defending against fraud, but if this sensitive information falls into the wrong hands in your system, it could lead to losing your customers' trust and perhaps even require you to defend yourself in a lawsuit. Safeguarding personal information is plain good business!*

8) Maintain Your Standards Post Onboarding

In transportation, things change all the time. It is important to put processes in place to maintain your high standards past onboarding. By doing this you help to reduce and catch fraud in your network. You will be able to identify fraud that can occur on a shipment better by consistently and continuously vetting the carriers in your network.

- Leverage your fraud prevention framework not only when onboarding carriers but for continued monitoring as carrier information can change daily.
- Create a method to check carrier information that meets your standards prior to assigning them to a load. Depending on the size of your operation this could be a manual check or a fully automated check through technology.
- If the load you are assigning to a carrier is going to be picked up at a later date, you can also employ the same manual or automated check the day of pickup to make sure the carrier still meets your standards.
- Develop an in-house set of metrics to measure your company's performance relative to your customers' demands and how carriers perform while hauling your customer's freight.
- Example of Performance Measurements: On-time pickup and delivery, and providing proper shipment documentation.
- Find a way to track these metrics objectively, leverage software or in-house methods. This will allow you to have fair and transparent conversations with carriers.
- Develop a method to let carriers know how they are performing and the rewards or consequences for meeting or not meeting standards.
- Create a "do not use" list for carriers who do not meet your service needs, or your selection criteria.
- Find a way to systematically note when carriers are on this "do not use" list to ensure the carrier is not reactivated at a later date or by another team member.

III. Collaborate With Shippers

The best way to limit fraud and theft on loads is to collaborate closely with your customers. They have a vested interest in making sure the load runs smoothly and they can help you reduce fraud in the industry. Before moving loads with a customer, understand their best practices and feel comfortable sharing a list of how you've been successful with other customers. Some steps to incorporate or suggest to shippers include:

- Verify with the shipper/consignee that the load has been picked up and delivered.
- Require shipment paperwork is used (BOL).
- Confirm trucking company name with shipper.

- Instruct shippers to turn away drivers using temporary placards on trucks or trailers. This should be an immediate red flag.
- Inspect for removable nut and bolt attachment instead of safety nut assembly on trailer doors and reject trailers with removable nut and bolt attachments.
- Note the seal number and color on the BOL.
- Suggest seals that are more difficult to tamper with or recreate with 3D printers.
- Some shippers are now taking pictures of the truck that picked up the freight, including door placards and license plates, and are asking receiving facilities to take pictures upon delivery so the pictures can be compared and if seals or trailers have been switched. Request pictures if available.
- Work with shippers to understand which of their facilities are in higher risk areas for theft. Use this information to inform carrier selection and increased security practices in the area.
- Have shippers obtain and provide you with the VIN of the tractor picking up. This enables you to confirm that such tractor is included under the carrier's cargo insurance policy.

A. Fradulent Shippers

While rare, there have been instances of fraudulent shippers using brokers to move freight and then defaulting on payments. Prior to working with a customer, run a credit check and request information to verify that they are a legitimate company. As part of this process, confirm that email domains match exactly the email address of the company. Often, the authentic email domains will match the purported customers website domain. These types of "purported customer" frauds are becoming more prevalent.

B. Other Aspects of a Shipment That Experience Fraud

While most scenarios facing fraud have been covered by the above recommendations, there are other aspects of a shipment that can experience fraud. It is important to partner with both the carrier and shipper to help reduce the occurrence of these examples:

Double-Brokering

By using track and trace technology you can see if the carrier assigned to the load is truly hauling it. If you are not seeing expected progress or experiencing inaccurate information from the carrier you can begin to investigate if double-brokering has occurred. In this case, be sure to pay the carrier that actually hauled the load to avoid double payments. It is also a good idea to review the number of USDOT inspections a carrier has experienced and compare the number of inspections with the number of power units reported through the carrier's MCS-150 report. This can be done at this FMCSA website (or through a number of available vendors): SAFER Web - Company Snapshot (dot.gov)

Unauthorized Load Consolidation

For shipments lower in weight and total volume, carriers may consolidate loads to increase overall payments for the load. This can result in a claim from your customer for load tampering. Be sure to work with your customer on proactive measures such as seals and limiting the information provided to the carrier prior to pick up.

Unauthorized Use of Intermodal

Carriers may use the rail to save costs on moving goods across the country. Be sure to work with your customer on proactive measures such as seals and information provided to the carrier prior to pick up. You can also use track and trace to ensure the load is moving by truck and not by rail.

Detention Fraud

There have been instances of carriers requesting detention payments for time not spent waiting to be loaded or unloaded. Use BOL, track and trace, and partner closely with your customers to make sure detention payment requests are valid. Track detention requests to see if some carriers are requesting unusually high amounts of detention.

Lumper Payments

Be sure if you are providing reimbursement or advances for lumper payments the carrier has completed the load. You can use BOL or location services to help verify this. It is also important to create limits on how often and the amount a carrier can ask for reimbursement. *Lumper receipts submitted to you are also a good source for determining what carrier actually transported a load and if the request for lumper reimbursement is valid.

Carrier Bypassing Factoring Company

If a carrier is stating they no longer have a relationship with their factoring company and want to be paid directly, request a letter of release directly from the factoring company.

POST-THEFT

Should the absolute worst happen, and the carrier entrusted with a shipment has stolen the cargo or failed to deliver services paid for, a broker could face a significant financial loss. Such an experience is a brutal lesson. Many technology tools have improved your chances of cargo theft recovery. Shippers are advised to include GPS trackers in their cargo that will always communicate its location. Post-theft recovery is the time when the return-on-investment shines. This section includes an anecdote as well as a list of tips and resources available to brokers to help brokers seek redress and protect their company name if they find themselves facing the consequences of a theft.

POST-THEFT ANECDOTE

The broker booked the carrier on a load-out trailer run from San Diego, CA, on July 1, 2019, to Laredo, TX, to arrive on July 11, 2019. The broker received a call from the carrier on July 11 that the brand new 2019 53' dry van trailer had gone missing along with the driver, and the carrier filed a missing person report with the Los Angeles Sheriff's Department. That same day, the broker learned that the carrier had picked up a load of cardboard coffee cans on July 1 in Norwalk, CA, and never showed up for delivery on July 5. The carrier confirmed that the now-missing trailer had been used to pick up this product in Norwalk, CA, a day after picking up the trailer in San Diego. Since the carrier had already filed a missing person report for the driver, the broker filed a report with CargoNet for the missing trailer and coffee cans. Per the carrier, on July 11 the police found the truck in Fontana, CA, but the trailer was not with it and they still could not locate the driver.

Over the next two weeks, the broker worked with CargoNet and the Los Angeles Sheriff's Department (LASD) to track down the driver and trailer. On July 24th, LASD contacted the broker and CargoNet to say they found the trailer and cargo at the driver's place of residence. LASD advised that most of the load, minus two cans, were recovered inside the trailer. The seal on the trailer was cut, and the trailer was recovered missing its exterior wheels and attached to a tractor stolen in a separate incident. At this time, the units were taken to a tow yard in Riverside, CA.

After sending an adjuster to the tow yard in Riverside, and having the trailer repaired, the broker was able to send a new carrier to pick up the trailer, properly dispose of the coffee cans, and deliver the trailer to the intended recipient in Laredo, TX, on August 26, 2019. The carrier, who was working with the broker to find the trailer, stopped communicating once the trailer was located, and the broker ended up paying all costs of the recovery.

IV. Member Suggested Post-Theft Recommendations

1. Check your technology! Ping your GPS devices, check notifications if a driver breached a geo-fence, consult with your track and trace service providers.
2. Speed is of the essence when dealing with theft. Treat every theft as if you have only 48 hours to recover your cargo. Report thefts immediately to improve your chances of recovery. Holding on to pride and/or reputation instead of reporting thefts can hinder your ability to recover your merchandise.
3. Services such as CargoNet may be able to find your stolen goods if they are posted on the dark web. If a perpetrator posts a picture of your products containing a RFID code, a search matching the RFID code should easily identify your goods.
4. Provide police investigators with all possible information, including pictures, information on the prior theft, and supplied invoices proving the value.
5. Stay in contact with the police – they are busy, and the squeaky wheels often do get helped first!
6. Insurance coverage is only triggered by specific events. Know your policy and the exclusions. If a carrier is being uncooperative during the insurance filing process, feel free to contact their insurance agent to expedite the process yourself.
7. Share information on untrustworthy companies and cultivate a reputation for taking the necessary steps to pursue wrongdoers. Post reports on TIA Watchdog and other technology solutions to spread the word.

V. Long-Term Post-Theft Planning

1. Establish clear post-theft protocols and define procedures for employees (ex: sample Incident Intake Form, Addendum 2):
    a. Who handles the “first report” and where do they go from there?
    b. Name of employee responsible for notifying your customer(s).
    c. Name of employee who will work directly with law enforcement.
    d. Name of employee who will coordinate claim(s) with insurance companies.
    e. Determine which employees will be responsible for different types of theft.
        - Third party cargo
        - Dishonest driver or fraudulent pick-up
        - Identity Theft
        - Financial Theft

2. Develop list of contact information and contact appropriate entities immediately:
    a. Local police, private investigators, and local task force.
    b. Your insurance agent.
    c. Fuel Advance - Security officer for your electronic check company.
    d. Financial Theft - Your bank security officers.
    e. Identity Theft - Credit reporting services, TIA, load boards, factoring companies, credit companies.
    f. Federal agencies, for example:
        - Hazardous Materials: Contact local FBI immediately.
        - Food: Department of Agriculture.
        - International: Department of Customs and Border Protection (CBP).
3. Contact the shipper to fill in any blanks on the shipment, so the victim has all the information for law enforcement to use in recovery.
4. Provide a scripted statement an individual can read to law enforcement to fully describe the exact nature of the theft and ensure it is understood. Include VIN number/make, truck/tag number, color of unit/marks on door. Including more detail improves the chances of finding the offender.
5. Describe what happened, what to look for, what phone, fax and email were used, and contact names.
6. Keep copies of any bogus paperwork in case it goes to court.
7. Be responsive, be involved, and be willing to invest time and financial resources.
8. Follow up frequently with attorneys and police officers.
9. Seek legal counsel to protect against any claims.
10. Network with industry to educate and improve best practices to fight theft.
11. Modify vetting processes, identify weaknesses, and learn from mistakes. Fictitious pickups are down as a direct result of improved carrier vetting practices in the industry.
12. Review corporate insurance policies to ensure coverage for monetary losses should the shipper or insurance company subrogate their losses against the broker.

POST-THEFT CONTACT INFORMATION

Transportation Intermediaries Association	(703) 299-5700
Report Theft to TIA Watchdog	https://www.tiawatchdog.com/login/
Industry Load Boards	https://tia.officialbuyersguide.net/
CargoNet	(888) 595-2638 | cargotheft@cargonet.com
Federal Bureau of Investigation	https://www.fbi.gov/contact-us/field-offices
State Law Enforcement Task Forces	See Addendum 1 for Contact Information
Internet Truckstop	security@truckstop.com
DAT	(800) 848-2546 | nacustomerservice@transcore.com
Registry Monitoring	n.anderson@registrymonitoring.com
Ansonia Credit Data	(877) 218-2056 | tsulpizio@ansoniacreditdata.com
Carrier 411	(321) 286-5171 | support@carrier411.com

DEPENDING ON TYPE OF THEFT, ALERT…

Cargo Theft	Insurance Company, State & Local Police, Private Investigators, TIA, CargoNet and load boards
Hazardous Materials	Insurance Company, Local FBI Field Office
Food	Insurance Company, U.S. Department of Agriculture, U.S. Department of Transportation Inspector General
International Freight	Insurance Company, U.S. Customs & Border Protection
Financial Theft	Insurance Company, Your Bank's Security Officers
Fuel Advance	Insurance Company, Security Officer for Your Electronic Check Company
Identity Theft	Insurance company, credit reporting services, FMCSA, TIA, and load boards

SECTION 3: RESOURCES

I. **State & Local Law Enforcement Cargo Theft Task Forces Investigator Contact Information**

II. **Sample Incident Intake Form**

III. **Fraudulent Insurance Certificates**

IV. **Fraudulent MC Authority / Valid FMCSA Carrier Information**

I. State & Local Law Enforcement Cargo Theft Task Forces Investigator Contact Information

CALIFORNIA

Los Angeles County Sheriff's Department – "CARGOCATS"

Lieutenant Craig Ditsch
(562) 946-7268

Sergeant Mike Trujillo
matrujil@lasd.org
Office: (310) 603-3138
Cell: (310) 678-4353

Detective Chae Song
Cell: (310) 678-3910

Crime Analyst Shellise Berry
(562) 946-7250
Cell: (562) 522-7684

California Highway Patrol Cargo Theft Interdiction Program – "CTIP"

SOUTHERN DIVISION – LOS ANGELES

Main Number: (310) 513-7800

Sergeant Sid Belk
sbelk@chp.ca.gov
Office: (310) 513-7810
Cell: (951) 5338

Detective Larry Myhre
lmyhre@chp.ca.gov
Cell: (310) 513-7819

Detective Byron Culberson
bculberson@chp.ca.gov
Cell: (310) 505-9001

Sergeant Amador Portillo
Cell: (619) 572-6954

Analyst Merri Hawkins
mhawkins@chp.ca.gov
(310) 513-7800

Theft Report Website
www.chp.ca.gov/html/ctiphowtoreport.html
Loss information only disseminated to law enforcement agencies

NORTHERN DIVISION – OAKLAND

Sergeant Ward Radelich
WRadelich@chp.ca.gov
Office: (510) 622-4614
Cell: (510) 715-6529

San Francisco International Airport – "AIRCATS" - San Francisco Police Department

Detective Mike Etcheverry
Office: (650) 821-5268
Cell: (650) 483-6852

Los Angeles Police Department – "BADCATS" - Commercial Crimes Division

Detective Mark Zavala
23740@lapd.lacity.org
Office: (213) 847-3786
Cell: (213) 268-0819

Detective Matt Sibayan
30196@lapd.lacity.org
Office: (213) 847-3786
Cell: (213) 399-0103

Los Angeles Police Department – LAX Airport Crimes Unit

Detective Richard Householder
Detective Jesse Ortiz
(310) 348-3931

FLORIDA

Florida Statewide Cargo Theft Task Force
Florida Highway Patrol

Lieutenant Tony Bartolome
Bartolome.tony@fhp.hsmv.state.fl.us
(407) 858-3233

Corporal David Vincent
Vincent.david@fhp.hsmv.state.fl.us
(352) 732-1260

Theft Report Website
https://reportcargotheft.fhp.state.fl.us
Loss information only disseminated to law enforcement agencies

Marion County Sheriff's Office Task Force

Sergeant Mark Jones
mjones@sheriff.marioncountyfl.org
(352) 732-9111
(352) 368-3542

Detective Eric Dice
edice@marionso.com
Cell: (352) 843-2655

Florida Highway Interdiction Assistance

Allen Davis
davisa@doacs.state.fl.us

Office of Agriculture Law Enforcement

DEA Task Force
3384 Capital Circle, NE
Tallahassee, FL 32308
(850) 942-8417, DEA

Jacksonville Sheriff's Department

Detective David Scott
david.scott@jaxsheriff.org
(904) 630-2173

Sergeant Troy Rhodes
Troy.rhodes@jaxsheriff.org
(904) 630-2173
Cell: (904) 710-1169

Detective Kevin Mesh
Kevin.mesh@jaxsheriff.org
(904) 630-2174
Cell: (904) 874-6742

Miami-Dade Police Department

Lieutenant Luis Almaguer
U302669@mdpd.com
(305) 471-2624

Sergeant Carlos Rosario
U304470@mdpd.com
(305) 471-3374

Detective Ricardo Silverio
U305641@mdpd.com
(305) 471-2746

Detective Reward Reyes
U305356@mdpd.com
(305) 471-3631

Miami Federal Bureau of Investigation

Special Agent Alex Peraza
Office: (954) 392-7858
Cell: (954) 553-3639

GEORGIA

Georgia Cargo Task Force

SAC John Cannon
john.cannon@gbi.ga.gov
(404) 201-8476

SA Cecil Hutchins
cecil.hutchins@gbi.ga.gov
(678) 859-3627

SA Anita Ivy
anita.ivy@gbi.ga.gov
(404) 604-6951

SA Mark Lavender
mark.lavender@gbi.ga.gov
(706) 690-1323

TFA Thom Mobbs
thom.mobbs@gbi.ga.gov
(404) 503-0251

IA Denise Robertson
denise.robertson@gbi.ga.gov
(404) 503-7210

TFA Leslie Smith
leslie.smith@usdoj.gov
(404) 391-5913

TFA Charles Warrant
charles.warrant@usdoj.gov
(404) 391-5911

CIA Laurie Lane – Intelligence
laurie.lane@gisac.gbi.ga.gov
Direct: (404) 486-6448
Office: (770) 918-6772

Georgia Cargo Theft Alert System

https://www.gacargotheft.com

ILLINOIS

Tri-County Auto Theft Task Force – Chicago

Inspector Draksler
tricounty@wilicosheriff.com
(815) 727-5058

Mid-West Cargo Task Force - Illinois State Police Zone 3 Joliet Investigations Midwest Cargo Theft Unit

M/Sergeant Tony Zurek
zurekan@iso.state.il.us
(815) 726-6377 ext. 208
Fax: (815) 726-3312
Cell: (312) 969-2117

S/A Tom Vagasky
vagaskt@iso.state.il.us
Cell: (815) 641-4743

S/A Chris Linares
Linarec@isp.state.il.us
Cell: (815) 641-3738

S/A Jorge Foneca
Fonsecj@isp.state.il.us
Cell: (815) 641-4626

INDIANA

FBI New Albany/Indianapolis

Special Agent Paul Meyer
Office: (812) 948-8002
Cell: (502) 558-0532

KENTUCKY

Kentucky State Police

Sergeant Bobby Motley
Bobby.motley@ky.gov
(606) 776-7383

Louisville Metro Police Department

Sergeant Steve Hall
Steve.hall@louisvilleky.gov
(502) 574-4640

Federal Bureau of Investigation – Lexington, KY

Special Agent John Whitehead
hwhitehead@ic.fbi.gov (606) 254-4038

NEVADA

Las Vegas Metropolitan Police Department – VIPER (Auto & Cargo) Task Force

Lisa Pope
(702) 828-1966

Sergeant Richter
(702) 828-0105

Sergeant Chad Brown
(702) 828-5766

NEW JERSEY

Waterfront Commission of NY and NJ Major Case Squad

Captain Pete Massa
pmassa@waterfrontcommission.org
(973) 817-7798

New York City Police Department
Major Crimes Unit

Sergeant Buddy Murnane
Francis.murnane@nypd.org
Office: (716) 265-7327
Cell: (347) 672-2540

John F. Kennedy International Airport - KAT-NET Cargo Theft Task Force

PANYNJ PD Detective Patricia Lind
plind@panynj.gov
Office: (718) 244-4416

PANYNJ PD Detective Frank Crimarco
fcrimarco@panynj.gov Office: (718) 244-4363

Brooklyn-Queens Federal Bureau of Investigations Office

PANYNJ PD Detective Frank Esposito
Frank.esposito@ic.fbi.gov (718) 286-7842

Suffolk County Police Department

Sergeant Robert Doyle
doylerob@suffolkcounty.gov
(631) 852-6295

NORTH CAROLINA

Charlotte/Greensboro

FBI SA Doug Rentz
drentz1@leo.gov
(336) 855-7770

PENNSYLVANIA

Pennsylvania State Police

CENTRAL/EASTERN

WESTERN

Sergeant Jeff Fisher
jefisher@state.pa.us
(412) 475-0911

SOUTHEAST

CPL Mike King
miking@state.pa.us
(484) 340-3617

CPL Brian Sarafinko
bsarafinko@state.pa.gov
(570) 963-4320
Cell: (570) 760-4925

Sergeant Rusty Fisher
dafisher@state.pa.us
(717) 443-6525

TENNESSEE

Nashville Metro Police

Detective Chuck Tarwater
chuck.tarwater@memphistn.gov
Cell: (901) 508-0462

Memphis Auto/Cargo Theft Task Force – "TAMCATS"

Federal Bureau of Investigation Office
(901) 747-4300

Memphis Police Department

Detective Alvin Clark
alvin.e.clark@memphistn.gov
Cell: (901) 508-1882

Detective Drew Hardin
james.hardin@memphistn.gov
Cell: (901) 258-0896

Shelby County Sheriff's Office

Barry Clark
Cell: (901) 508-0466

Shelby County Sheriff's Office Alert Unit
(901) 545-2800

Lieutenant Richard Nelson
Office: (901) 385-4716

Department Auto Theft Unit

Detective Robert Bristol
robert.bristol@nashville.gov
(615) 862-7612

Detective William Dillon
bill.dillon@nashville.gov
(615) 862-7610

Detective James Brown
james.k.brown@nashville.gov
(615) 862-7614

Detective Brandon Hazzard
david.hazzard@nashville.gov
(615) 862-7266

TEXAS

Texas Department of Public Safety – Garland, TX

Agent John Murphy
J.Murphy@dps.texas.gov
Office: (214) 861-2255
Cell: (214) 850-3701

Agent Patrick Hentz
Patrick.Heintz@dps.texas.gov
Office: (214) 861-2000
Cell: (214) 205-2794

Dallas Police Department Cargo Theft Unit

Detective Ed Matis
edward.matis@dpd.ci.dallas.tx.us
Cell: (214) 329-8978

Detective Ed Anaya
edward.anaya@dpd.ci.dallas.tx.us
Cell: (214) 329-8970

Fort Worth Police Department

Sergeant Clay Hays
Clayton.hays@fortworthgov.org
(817) 944-9047

Detective Ivy Haley
Ivette.haley@fortworthgov.org
(817) 392-4415

Houston Police Department - Major Offenders Unit

Detective Alfredo Mares
Alfredo.Mares@cityofhouston.net
Cell: (832) 314-6030

Detective David Vasquez
David.Vasquez@cityofhouston.net
(713) 484-9065

UTAH

West Valley City Police Department

Detective Holly Ziegenhorn
holly.ziegenhorn@wvc-ut.gov
(801) 209-7623

RAILROAD POLICE

Union Pacific Railroad Los Angeles, CA

Igor Pisnoy
iapisnoy@up.com
(323) 353-0509
El Paso, TX

Larry Diaz
ldiaz@up.com
(915) 727-9753

Burlington Northern Santa Fe Railroad

Chief Special Agent Chuck Matthews
Charles.Matthews@bnsf.com
(817) 565-3010

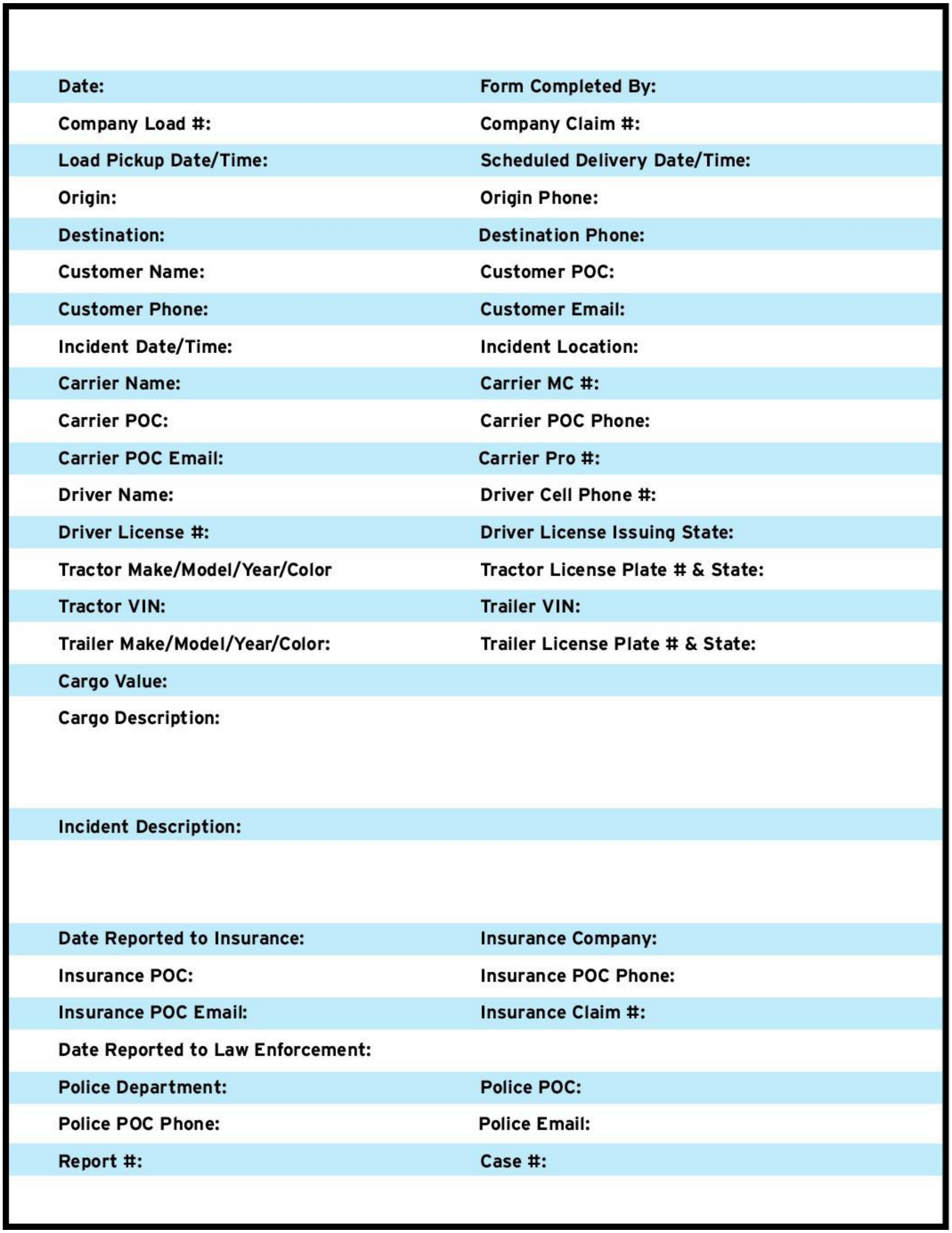
CSX Railroad

SSA Patrick Hemphill
Jp_Hemphill@csx.com
(904) 625-0871

Norfolk Southern Railroad

SSA Richie Vaughan
Richard.Vaughan@nscorp.com
(908) 820-2605

II. Sample Incident Intake Form



Date:	Form Completed By:
Company Load #:	Company Claim #:
Load Pickup Date/Time:	Scheduled Delivery Date/Time:
Origin:	Origin Phone:
Destination:	Destination Phone:
Customer Name:	Customer POC:
Customer Phone:	Customer Email:
Incident Date/Time:	Incident Location:
Carrier Name:	Carrier MC #:
Carrier POC:	Carrier POC Phone:
Carrier POC Email:	Carrier Pro #:
Driver Name:	Driver Cell Phone #:
Driver License #:	Driver License Issuing State:
Tractor Make/Model/Year/Color	Tractor License Plate # & State:
Tractor VIN:	Trailer VIN:
Trailer Make/Model/Year/Color:	Trailer License Plate # & State:
Cargo Value:	
Cargo Description:	
Incident Description:	
Date Reported to Insurance:	Insurance Company:
Insurance POC:	Insurance POC Phone:
Insurance POC Email:	Insurance Claim #:
Date Reported to Law Enforcement:	
Police Department:	Police POC:
Police POC Phone:	Police Email:
Report #:	Case #:

III. Fraudulent Insurance Certificates

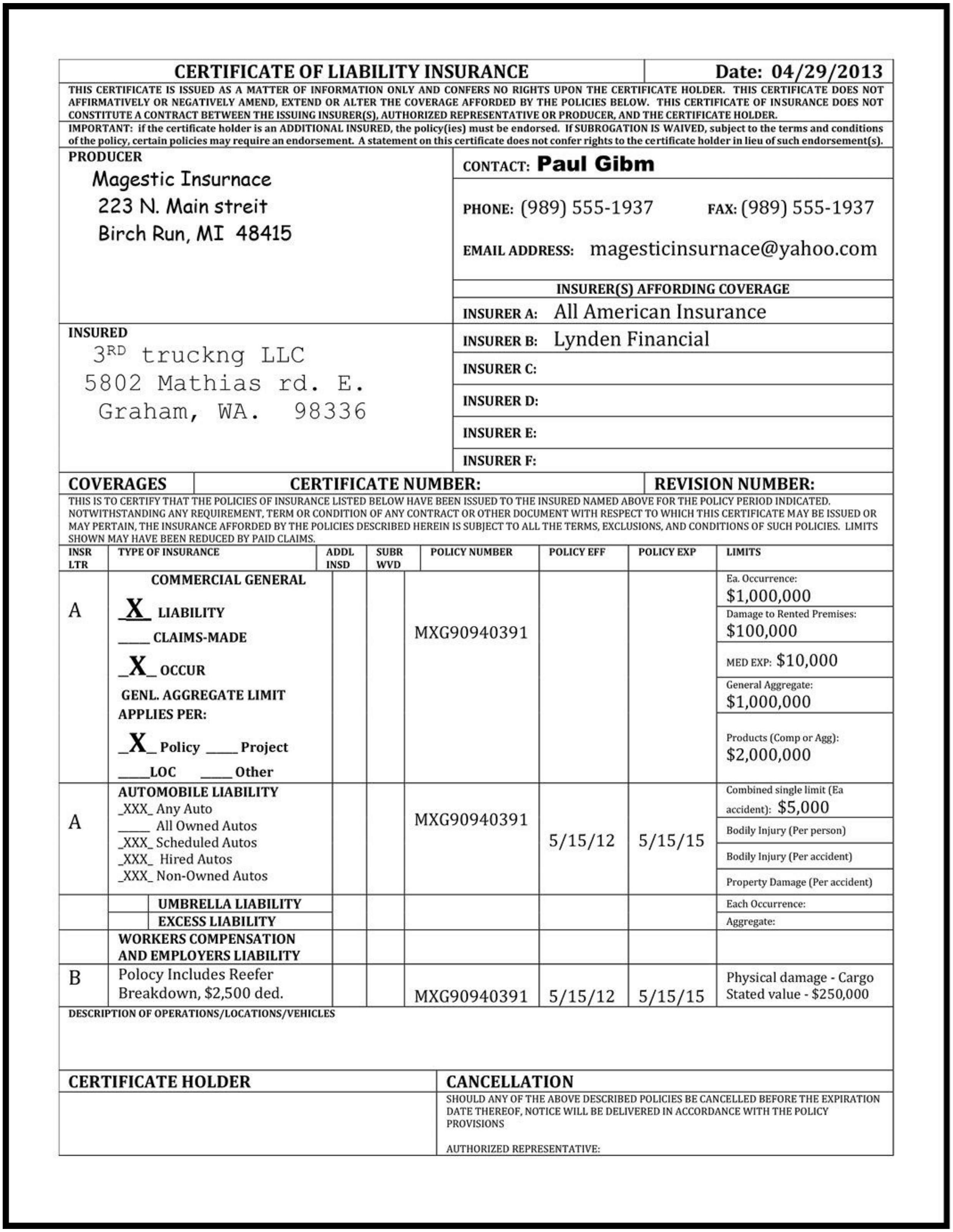
On the following pages are examples of fraudulent insurance documentation. Keeping in mind the recommendations of the checklists presented in the Framework to Combat Fraud, do any details of these certificates stand out?

Remember these important points in reviewing all carrier insurance and operating authority documents:

- Verify phone numbers and addresses.
- Few reputable insurance companies will use a free advertising-supported or a commercially available email account domain such as @gmail.com, @yahoo.com, or @earthlink.net.
- Make sure the name of the carrier matches the FMCSA licensing website.
- Make sure the name of the insurance company, policy number, and effective dates match the FMCSA licensing website.
- Valid certificates have consistent fonts.
- Look for an unusual font.
- Check for obvious spelling errors.

In addition to insurance documents, do not forget to also review the operating authority history on FMCSA's website. Carriers in financial distress may show multiple "involuntary revocations" and reinstatements of authority due to lapses in insurance coverage.

If you are able to identify details that merit additional investigation, or non-use of the carrier, what procedure does your company have in place for fraud prevention and response?



CERTIFICATE OF LIABILITY INSURANCE

Date: 04/29/2013

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: if the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER

Magestic Insurnace
223 N. Main streit
Birch Run, MI 48415

CONTACT: **Paul Gibm**

PHONE: (989) 555-1937 **FAX:** (989) 555-1937

EMAIL ADDRESS: magesticinsurnace@yahoo.com

INSURER(S) AFFORDING COVERAGE

INSURER A: All American Insurance
INSURER B: Lynden Financial
INSURER C:
INSURER D:
INSURER E:
INSURER F:

INSURED

3RD truckng LLC
5802 Mathias rd. E.
Graham, WA. 98336

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS, AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF	POLICY EXP	LIMITS
A	COMMERCIAL GENERAL _X_ LIABILITY ____ CLAIMS-MADE _X_ OCCUR GENL. AGGREGATE LIMIT APPLIES PER: _X_ Policy ____ Project ____LOC ____ Other			MXG90940391			Ea. Occurrence: $1,000,000 Damage to Rented Premises: $100,000 MED EXP: $10,000 General Aggregate: $1,000,000 Products (Comp or Agg): $2,000,000
A	AUTOMOBILE LIABILITY _XXX_ Any Auto ____ All Owned Autos _XXX_ Scheduled Autos _XXX_ Hired Autos _XXX_ Non-Owned Autos			MXG90940391	5/15/12	5/15/15	Combined single limit (Ea accident): $5,000 Bodily Injury (Per person) Bodily Injury (Per accident) Property Damage (Per accident)
	UMBRELLA LIABILITY EXCESS LIABILITY						Each Occurrence: Aggregate:
	WORKERS COMPENSATION AND EMPLOYERS LIABILITY						
B	Polocy Includes Reefer Breakdown, $2,500 ded.			MXG90940391	5/15/12	5/15/15	Physical damage - Cargo Stated value - $250,000

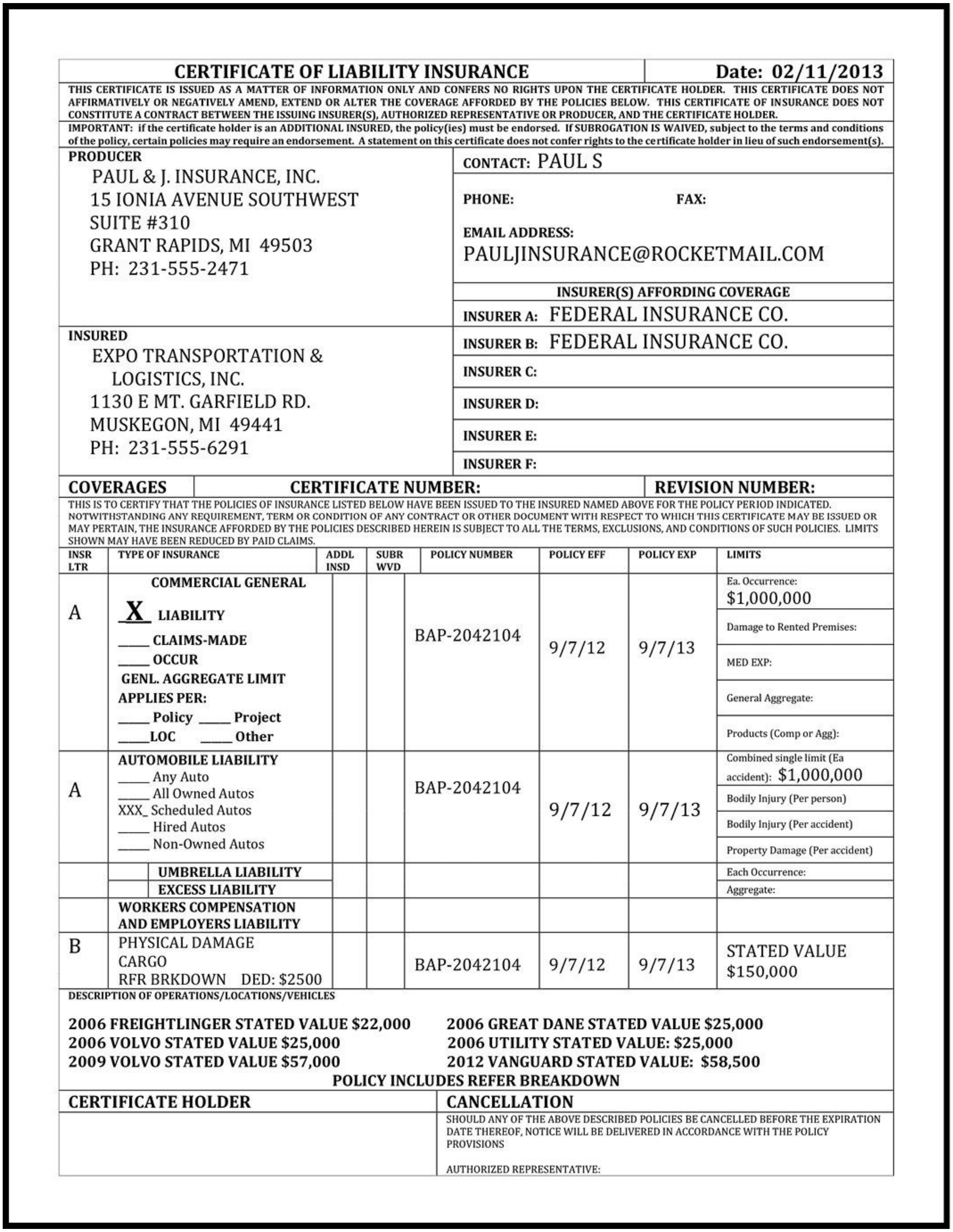
DESCRIPTION OF OPERATIONS/LOCATIONS/VEHICLES

CERTIFICATE HOLDER

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS

AUTHORIZED REPRESENTATIVE:



CERTIFICATE OF LIABILITY INSURANCE

Date: 02/11/2013

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: if the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER

PAUL & J. INSURANCE, INC.
15 IONIA AVENUE SOUTHWEST
SUITE #310
GRANT RAPIDS, MI 49503
PH: 231-555-2471

CONTACT: PAUL S

PHONE: **FAX:**

EMAIL ADDRESS:
PAULJINSURANCE@ROCKETMAIL.COM

INSURER(S) AFFORDING COVERAGE

INSURER A: FEDERAL INSURANCE CO.
INSURER B: FEDERAL INSURANCE CO.
INSURER C:
INSURER D:
INSURER E:
INSURER F:

INSURED

EXPO TRANSPORTATION &
LOGISTICS, INC.
1130 E MT. GARFIELD RD.
MUSKEGON, MI 49441
PH: 231-555-6291

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS, AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF	POLICY EXP	LIMITS
A	COMMERCIAL GENERAL X LIABILITY ____ CLAIMS-MADE ____ OCCUR GENL. AGGREGATE LIMIT APPLIES PER: ____ Policy ____ Project ____LOC ____ Other			BAP-2042104	9/7/12	9/7/13	Ea. Occurrence: $1,000,000 Damage to Rented Premises: MED EXP: General Aggregate: Products (Comp or Agg):
A	AUTOMOBILE LIABILITY ____ Any Auto ____ All Owned Autos XXX_ Scheduled Autos ____ Hired Autos ____ Non-Owned Autos			BAP-2042104	9/7/12	9/7/13	Combined single limit (Ea accident): $1,000,000 Bodily Injury (Per person) Bodily Injury (Per accident) Property Damage (Per accident)
	UMBRELLA LIABILITY EXCESS LIABILITY						Each Occurrence: Aggregate:
	WORKERS COMPENSATION AND EMPLOYERS LIABILITY						
B	PHYSICAL DAMAGE CARGO RFR BRKDOWN DED: $2500			BAP-2042104	9/7/12	9/7/13	STATED VALUE $150,000

DESCRIPTION OF OPERATIONS/LOCATIONS/VEHICLES

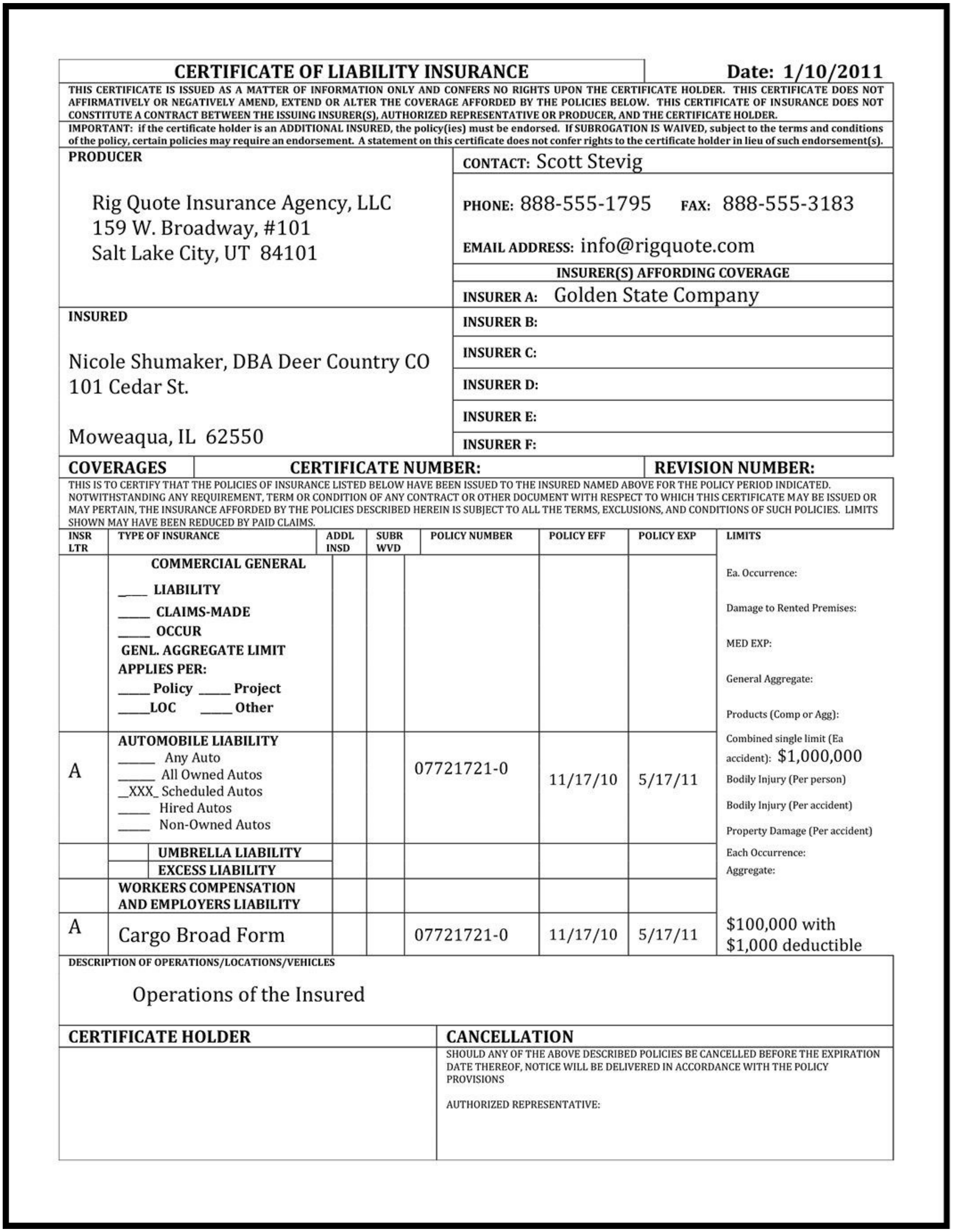
2006 FREIGHTLINGER STATED VALUE $22,000
2006 VOLVO STATED VALUE $25,000
2009 VOLVO STATED VALUE $57,000
2006 GREAT DANE STATED VALUE $25,000
2006 UTILITY STATED VALUE: $25,000
2012 VANGUARD STATED VALUE: $58,500
POLICY INCLUDES REFER BREAKDOWN

CERTIFICATE HOLDER

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS

AUTHORIZED REPRESENTATIVE:



CERTIFICATE OF LIABILITY INSURANCE

Date: 1/10/2011

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: if the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER

Rig Quote Insurance Agency, LLC
159 W. Broadway, #101
Salt Lake City, UT 84101

CONTACT: Scott Stevig

PHONE: 888-555-1795 **FAX:** 888-555-3183

EMAIL ADDRESS: info@rigquote.com

INSURER(S) AFFORDING COVERAGE

INSURER A: Golden State Company

INSURER B:

INSURER C:

INSURED

Nicole Shumaker, DBA Deer Country CO
101 Cedar St.

Moweaqua, IL 62550

INSURER D:

INSURER E:

INSURER F:

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS, AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF	POLICY EXP	LIMITS
	COMMERCIAL GENERAL ____ LIABILITY ____ CLAIMS-MADE ____ OCCUR GENL. AGGREGATE LIMIT APPLIES PER: ____ Policy ____ Project ____LOC ____ Other						Ea. Occurrence: Damage to Rented Premises: MED EXP: General Aggregate: Products (Comp or Agg):
A	AUTOMOBILE LIABILITY _____ Any Auto _____ All Owned Autos _XXX_ Scheduled Autos ____ Hired Autos ____ Non-Owned Autos			07721721-0	11/17/10	5/17/11	Combined single limit (Ea accident): $1,000,000 Bodily Injury (Per person) Bodily Injury (Per accident) Property Damage (Per accident)
	UMBRELLA LIABILITY EXCESS LIABILITY						Each Occurrence: Aggregate:
	WORKERS COMPENSATION AND EMPLOYERS LIABILITY						
A	Cargo Broad Form			07721721-0	11/17/10	5/17/11	$100,000 with $1,000 deductible

DESCRIPTION OF OPERATIONS/LOCATIONS/VEHICLES

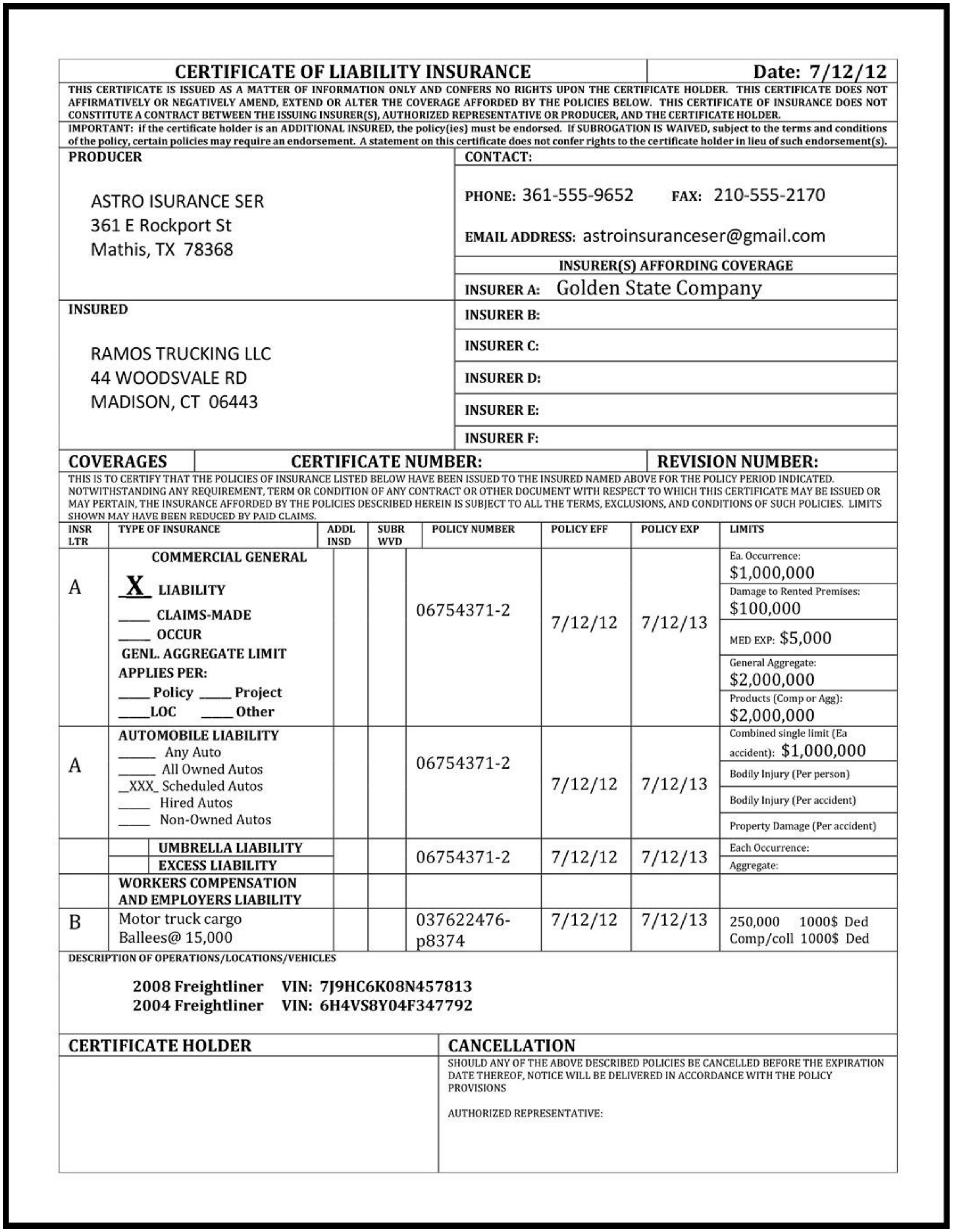
Operations of the Insured

CERTIFICATE HOLDER

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS

AUTHORIZED REPRESENTATIVE:



CERTIFICATE OF LIABILITY INSURANCE

Date: 7/12/12

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: if the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER

ASTRO ISURANCE SER
361 E Rockport St
Mathis, TX 78368

CONTACT:

PHONE: 361-555-9652 **FAX:** 210-555-2170

EMAIL ADDRESS: astroinsuranceser@gmail.com

INSURER(S) AFFORDING COVERAGE

INSURER A: Golden State Company

INSURER B:

INSURER C:

INSURER D:

INSURER E:

INSURER F:

INSURED

RAMOS TRUCKING LLC
44 WOODSVALE RD
MADISON, CT 06443

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS, AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF	POLICY EXP	LIMITS
A	COMMERCIAL GENERAL X LIABILITY ____ CLAIMS-MADE ____ OCCUR GENL. AGGREGATE LIMIT APPLIES PER: ____ Policy ____ Project ____LOC ____ Other			06754371-2	7/12/12	7/12/13	Ea. Occurrence: $1,000,000 Damage to Rented Premises: $100,000 MED EXP: $5,000 General Aggregate: $2,000,000 Products (Comp or Agg): $2,000,000
A	AUTOMOBILE LIABILITY _____ Any Auto _____ All Owned Autos _XXX_ Scheduled Autos _____ Hired Autos _____ Non-Owned Autos			06754371-2	7/12/12	7/12/13	Combined single limit (Ea accident): $1,000,000 Bodily Injury (Per person) Bodily Injury (Per accident) Property Damage (Per accident)
	UMBRELLA LIABILITY EXCESS LIABILITY			06754371-2	7/12/12	7/12/13	Each Occurrence: Aggregate:
	WORKERS COMPENSATION AND EMPLOYERS LIABILITY						
B	Motor truck cargo Ballees@ 15,000			037622476-p8374	7/12/12	7/12/13	250,000 1000$ Ded Comp/coll 1000$ Ded

DESCRIPTION OF OPERATIONS/LOCATIONS/VEHICLES

2008 Freightliner VIN: 7J9HC6K08N457813
2004 Freightliner VIN: 6H4VS8Y04F347792

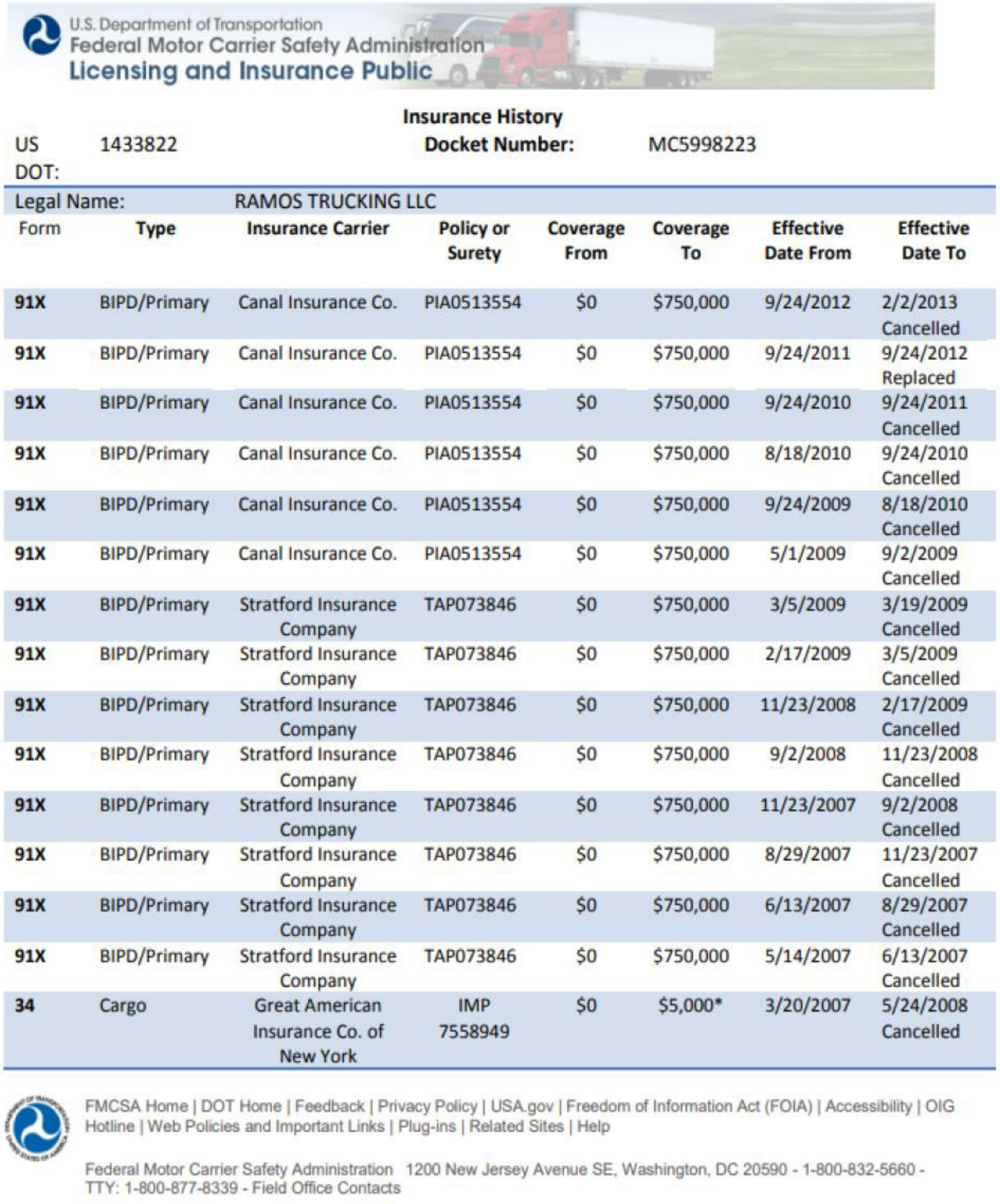
CERTIFICATE HOLDER

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS

AUTHORIZED REPRESENTATIVE:

IV. Fraudulent MC Authority / Valid FMCSA Carrier Information



U.S. Department of Transportation
Federal Motor Carrier Safety Administration
Licensing and Insurance Public

Insurance History

US DOT: 1433822 **Docket Number:** MC5998223

Legal Name: RAMOS TRUCKING LLC

Form	Type	Insurance Carrier	Policy or Surety	Coverage From	Coverage To	Effective Date From	Effective Date To
91X	BIPD/Primary	Canal Insurance Co.	PIA0513554	$0	$750,000	9/24/2012	2/2/2013 Cancelled
91X	BIPD/Primary	Canal Insurance Co.	PIA0513554	$0	$750,000	9/24/2011	9/24/2012 Replaced
91X	BIPD/Primary	Canal Insurance Co.	PIA0513554	$0	$750,000	9/24/2010	9/24/2011 Cancelled
91X	BIPD/Primary	Canal Insurance Co.	PIA0513554	$0	$750,000	8/18/2010	9/24/2010 Cancelled
91X	BIPD/Primary	Canal Insurance Co.	PIA0513554	$0	$750,000	9/24/2009	8/18/2010 Cancelled
91X	BIPD/Primary	Canal Insurance Co.	PIA0513554	$0	$750,000	5/1/2009	9/2/2009 Cancelled
91X	BIPD/Primary	Stratford Insurance Company	TAP073846	$0	$750,000	3/5/2009	3/19/2009 Cancelled
91X	BIPD/Primary	Stratford Insurance Company	TAP073846	$0	$750,000	2/17/2009	3/5/2009 Cancelled
91X	BIPD/Primary	Stratford Insurance Company	TAP073846	$0	$750,000	11/23/2008	2/17/2009 Cancelled
91X	BIPD/Primary	Stratford Insurance Company	TAP073846	$0	$750,000	9/2/2008	11/23/2008 Cancelled
91X	BIPD/Primary	Stratford Insurance Company	TAP073846	$0	$750,000	11/23/2007	9/2/2008 Cancelled
91X	BIPD/Primary	Stratford Insurance Company	TAP073846	$0	$750,000	8/29/2007	11/23/2007 Cancelled
91X	BIPD/Primary	Stratford Insurance Company	TAP073846	$0	$750,000	6/13/2007	8/29/2007 Cancelled
91X	BIPD/Primary	Stratford Insurance Company	TAP073846	$0	$750,000	5/14/2007	6/13/2007 Cancelled
34	Cargo	Great American Insurance Co. of New York	IMP 7558949	$0	$5,000*	3/20/2007	5/24/2008 Cancelled

FMCSA Home | DOT Home | Feedback | Privacy Policy | USA.gov | Freedom of Information Act (FOIA) | Accessibility | OIG Hotline | Web Policies and Important Links | Plug-ins | Related Sites | Help

Federal Motor Carrier Safety Administration 1200 New Jersey Avenue SE, Washington, DC 20590 - 1-800-832-5660 - TTY: 1-800-877-8339 - Field Office Contacts

TIA is the professional organization of the $343 billion third party logistics industry. TIA is the only organization exclusively representing transportation intermediaries of all disciplines doing business in domestic and international commerce. TIA is the voice of transportation intermediaries to shippers, carriers, government officials and international organizations. TIA is the United States member of the International Federation of Freight Forwarder Associations (FIATA).

TIA

1900 Duke Street, Suite 300
Alexandria, VA 22314
703.299.5700

www.tianet.org