2020 Framework to Combat Fraud

April 2020

Transportation Intermediaries Association
1625 Prince Street, Suite 200
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

Everyday 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 everyday, 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 Fraud Task Force Committee is comprised of a hand selected group of people with unique experience in their area of expertise. I'd like to thank the members of the 2014 Committee and those members who were integral in the development of this updated Framework.

My 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,

Mike Nervick CEO, Sleek Fleet, LLC.
Chair, TIA Fraud Task Force Committee

Members of the Working Group

Eric Airling, Integrity Express Logistics

Wade Anderson, Bay and Bay

Mark Boyer, CFI Logistics

Kari Dobrovolny, CTB, Pioneer Transfer

Keith Lewis, CargoNet

Dawn Mohler, CTB, GW Transportation Services

Mike Nerivck, Fleet Seek, LLC

Glenn Patton, Roanoke Insurance Group

Mike Sajdak, One Point Logistics

Lorin Seeks, Convoy, Inc.

Elise Van Vuren, Convoy, Inc.

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

CARGO THEFT

Fraud and Theft have gradually decreased in the last few years, however, the threat to the livelihoods of supply chain professionals is not eliminated. Criminals in the industry are being more selective in their targets and finding newfound sophistication using technology to enhance their schemes. The consequences of cargo theft reverberate throughout the industry as losses affect every part of a supply chain and ultimately raises 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. To be more specific, San Bernardino, CA, Los Angeles, CA, Dallas, TX, Cook County, IL, Miami-Dade FL counties top the charts for most common thefts in 2019.

Cargo theft costs small businesses, who already work on small profit margins, tens of billions of dollars a 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 in the industry arsenal to combat criminality. The hope of the TIA Fraud Task Force is 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 2017-2019 illustrates trends in cargo theft over those past three years. Food and beverage, household goods and electronics were the most common commodities stolen during that time frame.

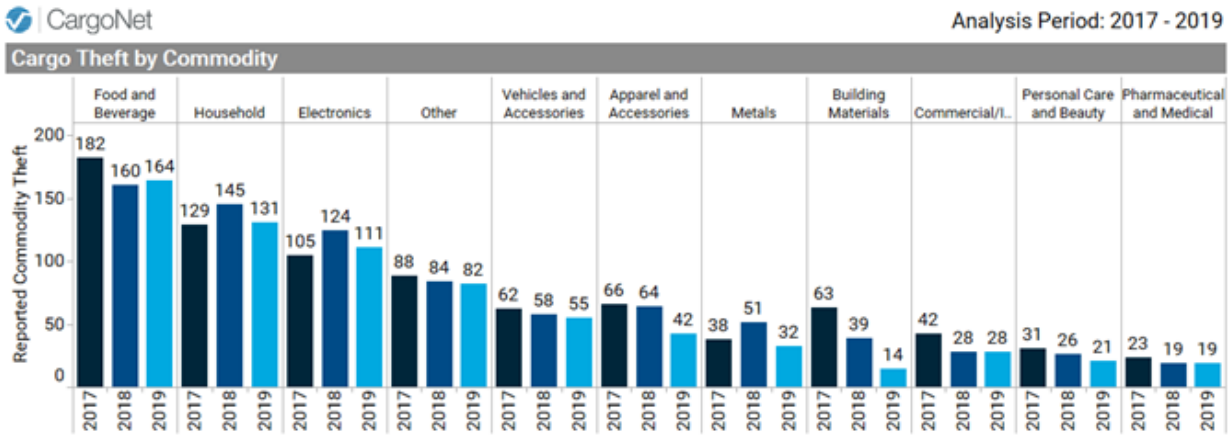

Fig. 1: Theft by Commodity 2017-2019, data courtesy of Verisk

The most common locations where thefts occurred were Warehouses/DC, truck stops, and from secured yards owned by carriers.

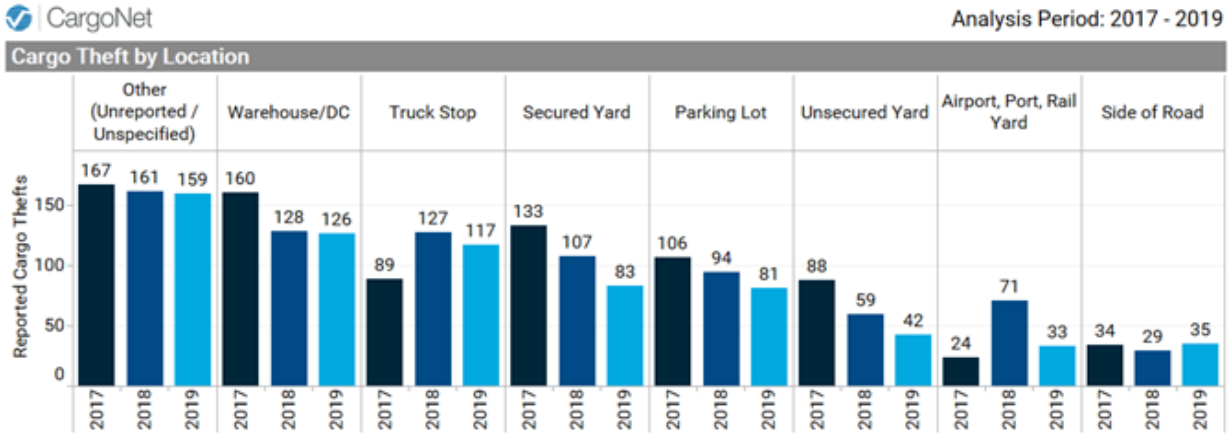

Fig. 2: Theft by Location 2017-2019, data courtesy of Verisk

Finally, data provided by Verisk shows that cargo thefts occur more often on Fridays and weekends, presumably because thieves recognize they will have more time before a theft is reported. Between 2017 and 2019, a maximum of 5% of thefts are reported on Saturday and Sunday. 95% of thefts are reported during the week, 25% on average reported on the Monday following a weekend theft.

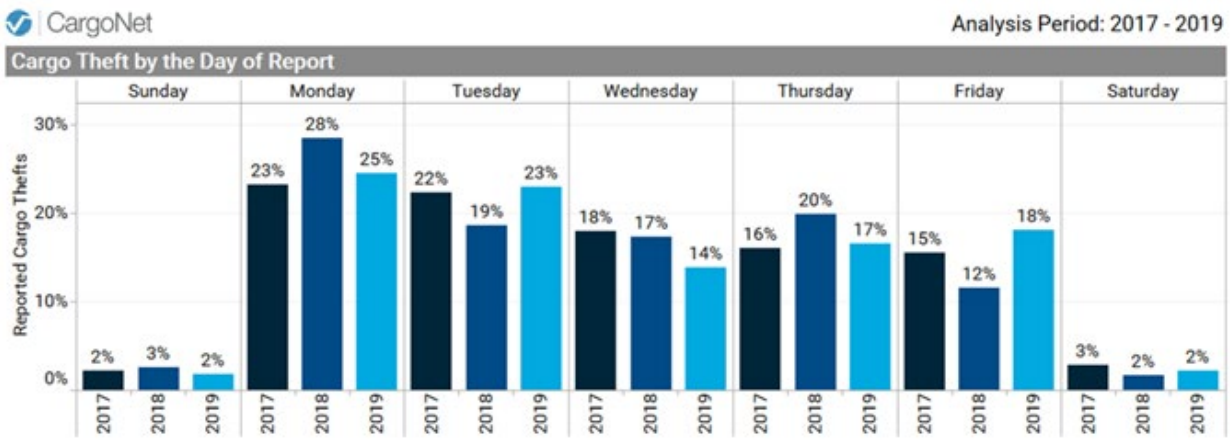

Fig. 3: Theft by Day of Week 2017-2019, data courtesy of Verisk

Cargo Theft Case Study #1:

One broker experienced vindictive behavior by a carrier they had used for several years. The carrier had run 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 was receiving less than quality communication 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 advised that they had plotted to steal this particular load as vengeance for the late fee from 2018; the load was then considered hostage. The brokerage met 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 for a cross-country delivery. 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.

It was revealed to the broker 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. Damages were incurred to the product and the customer took the load back from the broker to deliver the cargo themselves.

Cargo Theft Case Study #2:

On March 28, 2019, the Broker booked the Carrier on a load-out trailer move from Saginaw, TX to Laredo, TX. Per the rate confirmation, the trailer was to be picked up by Carrier on 3/28 and delivered on 4/4. Carrier told Broker that the trailer was delivered on 4/5/19. When informed by the receiver that the trailer never arrived, Broker was told by Carrier that the trailer would instead deliver on 4/11, then 4/12, and then again on 4/16 when Carrier called Broker stating they were finally checked in and waiting to unload. On 4/23, the Customer contacted the Broker stating that this trailer still has not arrived at the destination in Laredo, TX. From this point on, Carrier stopped answering all calls and e-mails.

After further investigation into the Carrier in possession of the Customer's trailer, it was uncovered that the insurance policy for 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, Broker sent a different driver to the address on file for Carrier to see if Broker could get in contact with someone in person. Broker was informed by this driver that Carrier's physical address on file is not actually their business and it was a bread shop instead. The only contact Broker made with Carrier in May was a phone call with one employee who claimed they could not speak English, and abruptly hung up.

During the investigation with Saginaw PD and CargoNet, it was determined that Carrier was a fraudulent company. There were 4 other companies associated with Carrier, linking multiple names and phone numbers to the same address that was the bread shop. All 4 other 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 this date, the trailer has not been recovered, and the files are still open with CargoNet and Saginaw PD.

Member-Suggested Checklist for Prevention

1. 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.

2. Do not rely on one technological tool; diversifying your technology service improves your odds of theft prevention. 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 which can be a lengthy process.

3. 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.

4. Read your insurance policy! Insurance coverage is only triggered by specific events. If the carrier was a fraud from the start, the insurance company will have no responsibility to honor any claim. Have your own insurance in place to protect your company, 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.

5. Speed is of the essence when dealing with theft. Treat every theft as if you only have 48 hours to recover. Report thefts immediately to improve your chances of recovery.

6. Make sure carrier paperwork is actually read, studied and verified. Clearly communicate your contract terms to carriers to prevent unforeseen issues.

7. Gather as much information as possible that might be useful to authorities in the event of an investigation (see Addendum 1, sample intake form). Valuable info includes a picture of driver’s license, 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 (truck/trailer), as well as vital information on the side of truck/trailers, rear of trailers, and the interior of trailers.

8. Request the carrier to 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.
9. Contact/Notify: Shippers, produce markets affected, industry trade guides, regional cargo theft groups, process agent, insurance, load boards, and credit reporting agencies.

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.

Financial Theft Case Study #1 (Advances):

A broker posts a load on the load boards, and is contacted by someone impersonating a legitimate carrier. When dispatched, the driver then creates a false bill of lading using information provided by the shipper. When the broker requests a copy of the pickup bill of lading, the fake bill is submitted and an advance is given to the impersonator. In most cases, the load is never picked up from the shipper.

Financial Theft Case Study #2 (Financial Stability):

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. Driver picked up the load and on the way to the consignee the truck broke down 3 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. Carrier was not cooperative through the whole transaction. The repair bill was in excess of $3700.00 and had to be paid by the broker.

Financial Theft Case Study #3 (Check Fraud):

A Broker mails a check to a Carrier. The check is intercepted by someone who copies the check and using modern scanning and printing technology, produces multiple checks with a "legitimate" signature and format and amounts. The checks often use numbers that are current to the Brokers account. These checks are then cashed (usually in batches) and by the time the Broker realizes the fraud, the perpetrators have moved on with the money. Depending on the Broker's agreement with their bank, they may be liable for the full amount. This happens most often around the holidays when Broker's staff may be on vacation or stretched thin.

Financial Theft Case Study #4 (Double Brokering):

A Broker tenders a load or loads to a small to midsize carrier. That carrier then takes the loads they accepted and brokers it out to another carrier, sometimes paying more money than they contracted for. The Initial carrier makes check calls back to the Broker and obtains a copy of the BOL and POD and forwards their invoice for payment. Months later, the Broker is advised that their carrier brokered the freight to someone else and did not pay for the actual carrier for the load. The original carrier is no longer in business and Collection agencies are going after the Broker's customer for payment.

Suggested Checklist for Prevention

1. Many brokers have stopped giving fuel advances or put in additional processes to limit advances..
2. Make sure any change to carrier information is validated. Contact verified 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, www.safersys.org, or to verify Texas intrastate DOT numbers, http://apps.txdmv.gov/apps/mccs/truckstop/).
6. Look at TIA Watchdog, Carrier 411 and DAT Directory 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 carriers financial stability by researching their credit history using a credit reporting service.

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.

Identity Theft Case Study #1:

A brokerage company begins receiving invoices from carriers for loads that do not show in the brokers' system. Some carriers have carrier load confirmations that show the broker company name, complete with an address and phone number that are similar to the broker's. However, those load confirmations are 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.

Identity Theft Case Study #2:

A new customer calls with three loads of product that needs to be moved. Credit is checked, customer credentials (address/phone) is verified and a contract is executed. The new customer contact states they work from home, so an alternative telephone number is provided for load updates. The loads pick up and deliver without issue. The loads are processed normally and carriers paid. When payment hasn't been received after 30 days, a collection call is made to the customer company where it was revealed that the customer has never heard of the broker and never authorized the loads to be transported. A call to the customer contact "home" phone shows the number as now disconnected. The consignee is a warehouse and the product is long gone.

Suggested Checklist for Prevention

1. Verify, verify, verify – know to the best of your abilities that you are dealing with a legitimate carrier/customer. If something doesn't match (like a phone number), check it out.
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 to go pick 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, the load boards, Internet Truckstop Security Department (security@truckstop.com), 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.

INTERNAL THEFT

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

INTERNAL THEFT CASE STUDY #1:

A small brokerage had limited administration 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 crime. The scheme 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. 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.

INTERNAL THEFT CASE STUDY #2:

An agent's contract is terminated for non-performance. A few months later, the brokerage receives several past-due invoices from a LTL broker for loads that don't match up with loads in the brokerage's TMS. After calling the LTL broker, the brokerage owner discovers 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 the account so 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/phone that was no longer valid.

Suggested Checklist for Prevention:

1. Run background checks on new employees or agents. Actually check 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 thing all the time. Not only will it help your office become more efficient, it will make it harder for employees to do nefarious things.
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.

DATA / INFORMATION THEFT

The importance and value of a company's information and data are 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.

Data Theft Case Study #1:

An employee at a brokerage receives an email with access to an internet-based shared file. The employee clicks on the link, installing ransomware on their computer, which spreads to the entire network. The ransomware shuts down the majority of critical systems, locking access to critical information to continue operations. An electronic ransom note demanding bitcoin payment to unlock systems and data replaces the information that existed only minutes prior to clicking the link in the suspicious email.

Data Theft Case Study #2

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

Data Theft Case Study #3

A bad actor working on behalf of a competitor drives into the parking lot and parks next to the building and jumps on an under-secured Wi-Fi network. From their car, this cybercriminal accesses network resources, copying customer and carrier contacts, along with pricing models and financial records.

Suggest Checklist for Prevention:

1. Ensure firewalls and Wi-Fi networks are secure, and tested periodically. Cybersecurity companies can 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. Build an Emergency Response Plan, including communication to stakeholders.

6. Test restoration and recovery of systems and data.

PREVENTION

Fraud and 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 the best carriers is not only important in providing world class service to your customer, but is also equally important in preventing major headaches down the road, and possible financial loss to both you (the broker) and your customer. This section will help you to understand the importance of having preventive measures in place, and help you to identify the necessary steps to protect the assets of your company.

Manage Your Own Risk and 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.

- **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 and only to verified recipients.
- **Use Contracts**. A signed contract provides a written guarantee between all parties that clarifies liability and provides recourse in courts. TIA strongly encourages members to use TIA's model contracts www.tianet.org.
- **Procure insurance** that supports the business you are currently running and planned growth. This insurance should also protect you from fraud induced liabilities that may arise within your business and from your shippers and carriers.
- **Create a carrier selection framework.** 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.
- Work with organizations that supply **cargo theft trends and data analytics** about cargo theft and fraud. Data is power and through the use of cargo theft analytics, one can better identify risks within their own scope of the supply chain. The information can be used to perform deep carrier history checks to be more selective about which carriers you hire to operate in areas of greater risk for theft and fraud. and to provide motor carriers with better information to avoid being the victim.

Thoroughly Vet and Maintain Your Carrier Network

Develop a Detailed Carrier Selection Framework

We recommend implementing written procedures when selecting carriers; you can use TIA's Carrier Selection Framework as a comprehensive model to create your own policy. While not verbatim, the section below provides an overview of carrier selection best practices. Additionally, there are many steps you can take to implement your framework, which we will cover.

Process for collecting and verifying carrier compliance information

- Collect information on operating authority and insurance directly from the carrier, then use a combination of the below sources to verify the accuracy of the information provided by the carrier:
    - Internet searches
    - FMCSA Website for Licensing and Insurance
    - FMCSA Safety and Fitness Electronic Record System (www.SaferSys.org)
    - Your own company database
    - Leverage 3rd-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 can help identify chameleon carriers, or setup their own monitoring tool leveraging the publically 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.

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.

Operating Authority

- Verify the authority granted by FMCSA.
- Common carriers are granted a "certificate" while contract carriers are granted a "permit," 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 Motor Carrier 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.
- Carriers in financial distress 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.

Insurance Documents

- Check the length of time that the carrier has had authority and insurance, and verify that their authority and insurance will cover any contracted pickup days.
- 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 name matches the FMCSA licensing website
- Validate 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 under-writing policies for the group. Typically, risk retention groups have very high deductibles and are geared more for medium (50+ trucks) sized carriers.

Carrier Safety Ratings (U.S.)

- Verify the carrier's safety rating at www.safersys.org, "Company Snapshot." If a carrier's safety rating is "Unsatisfactory," call the carrier's management and ask if the rating is correct. Verify the rating, and any updates, by calling FMCSA.
- 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. This is common as not all carriers receive audits that lead to Safety Ratings.

Carrier Safety Ratings (Canada)

- If applicable to the geographical scope of your operation (you contract with Candian carriers), Canadian carriers should meet your US Standards as well as the Canadian Safety stands 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 US.
- Leverage provincial 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 motor carrier is safe to operate in interstate commerce.
- Canadian motor carrier safety fitness determinations can be verified by navigating through www.safersys.org, or directly through the specific Canadian Province website.

Additional Items to Validate

- 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 beware of the following red flags:
    - Look for strange gaps in the carrier's authority history.
        - For example, if 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 simply because some brokers refuse to work with new carriers.
        - Consider the number of trucks the person is telling you the carrier operates. EXAMPLE: A carrier claims to have 1,000 trucks for a 2-month old MC number.
- As mentioned above, when validating paperwork is it important to verify 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 opened up another new MC. 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
    - Share the same or similar business address
    - Same phone number
    - Same owner/contact and email address
    - Similar VIN numbers for trucks used in the business

Utilize TIA Watchdog in Your Carrier Selection Process

- Check TIA Watchdog for any complaints or warnings about the carrier.
- Upon onboarding check the MC or DOT 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.

Collect Driver Information

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

- Purchase driver's license readers to scan licenses (if possible)
- Obtain a clean thumbprint from driver (if possible)
- Request a driver fax copies of his CDL and tractor/trailer registrations. This enables identity verification and ensures that the actual piece of 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.

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 still 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 the carrier to is a pickup on 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 to 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 or function 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 does not get reactivated at a later date or by another team member.

Partner with Shippers

The best way to limit fraud and theft on loads is to partner closely with your customers. They have vested interest in making sure the load runs smoothly and 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 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 with placards taped onto tractor. This should be an immediate red flag.
- Inspect for removable nut and bolt attachment instead of safety nut assembly
- 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. 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.

Fraudulent 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.

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 occurence 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.
- **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 pickup.
- **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 pickup. You can also leverage 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 for.
- **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:

Broker booked Carrier on a load-out trailer run from San Diego, CA on 7/1/19 to Laredo, TX on 7/11/19. Broker received a call from Carrier on July 11th, 2019 that the brand new 2019 53' dry van trailer had gone missing along with the driver, and Carrier filed a missing person report with the Los Angeles Sheriff's Department. That same day, Broker was made aware that Carrier picked up a load of cardboard coffee cans on 7/1 in Norwalk, CA and never showed up to delivery on 7/5. It was confirmed with Carrier that they used the now-missing trailer to pick up this product in Norwalk, CA a day after picking up the trailer in San Diego. Since Carrier had already filed a missing person report for the driver, Broker filed a report with CargoNet for the missing trailer and coffee cans. Per Carrier on 7/11/19, 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, Broker worked with CargoNet and Los Angeles Sheriff's Department to track down the driver and trailer. On 7/24/19, LASD contacted Broker and CargoNet stating 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 of 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 towed to a tow yard in Riverside, CA.

After sending an adjuster to the tow yard in Riverside and having the trailer repaired, 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 receiver in Laredo, TX on 8/26/19. Carrier, who was working with Broker to find the trailer, ceased all communication once the trailer was located and Broker ended up eating all costs of recovery.

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 only have 48 hours to recover. Report thefts immediately to improve your chances of recovery. Holding on to pride and/or reputation instead of reporting thefts eliminates your ability to recover your product.
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 FreightGuards and Trouble Reports where applicable such as on Carrier 411, Truckstop.com, and others.

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
        i. Third party cargo
        ii. Dishonest driver or fraudulent pick-up
        iii. Identity Theft
        iv. Financial Theft
2. Develop list of contact information and contact appropriate entities immediately:
    a. Local police, private investigators, local task force, TIA, security@truckstop.com, and CargoNet
    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:
        i. Hazardous Materials: Contact local FBI immediately
        ii. Food: Dept. of Agriculture
        iii. International: Dept. 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. More detail improves the chances of finding the offender.
5. Describe what happened, what to look for, what phone, fax and email were used, what 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 Assn.	(703) 299-5700
Report theft to TIA Watchdog	www.tiawatchdog.net/wdLogin.php
Industry Load Boards	tia.officialbuyersguide.net/SearchResult.asp?cid=33
CargoNet	(888) 595-2638 cargotheft@cargonet.com
Federal Bureau of Investigation	www.fbi.gov/contact-us/field
State Law Enforcement Task Forces	*See Addendum 1 for contact information*
Internet Truckstop	security@truckstop.com
Transcore/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 and local police, private investigators, TIA, Security@truckstop.com, and CargoNET
Hazardous Materials	Insurance company, local FBI office
Food	Insurance company, US Dept. of Agriculture, US Dept. of Transportation Inspector General, and Security@truckstop.com
International Freight	Insurance company, US Customs and Border Protection
Financial Theft	Insurance company, your bank security officers
Fuel Advance	Insurance company, security officer for your electronic check company, and Security@truckstop.com
Identity Theft	Insurance company, credit reporting services, TIA and Security@truckstop.com

RESOURCES

1) Law Enforcement Cargo Theft Task Forces contact information (9 pages)
2) Incident Intake Form (1 page)
3) Fraudulent insurance certificates (3 pages)
4) Fraudulent MC Authority/valid FMCSA carrier information (2 pages)

State & Local Law Enforcement Cargo Theft Task Forces
Investigators Contact Information

CALIFORNIA

L.A. 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, (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

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

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

TENNESSEE

Memphis Auto/Cargo Theft Task Force – "TAMCATS"

- Federal Bureau of Investigation Office: (901) 747-4300

- Shelby County Sheriff's Office
  - Barry Clark
    - Cell: (901) 508-0466

- 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 Alert Unit: (901) 545-2800

- Lieutenant Richard Nelson
  - Office: (901) 385-4716

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

Nashville Metro Police 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