The cargo theft prevention and recovery network

Cargo Theft by Fictitious Pickup

Keith Lewis, Vice President of Operations, CargoNet
Walt Beadling, Managing Partner, Cargo Security Alliance
EXECUTIVE SUMMARY

Cargo theft by fictitious pickup is a growing threat to supply chain security. A proliferation of information technologies enables thieves to defraud shippers and carriers at multiple points across the supply chain. This paper seeks to better define the terms and scope of this new supply chain cybercrime and provide seven best practices that can help prevent it.

DEFINITION

Fictitious pickups are criminal schemes that result in the theft of cargo by deception that includes truck drivers using fake IDs and/or fictitious businesses set up for the purpose of diverting and stealing cargo. Crimes of this type are also known as “fraudulent” or “deceptive” pickups, and the terms are used interchangeably. We’ve chosen to use the term “fictitious” because the perpetrators pick up cargo using false identification and/or fictitious carrier names and (in most cases) fence the stolen goods on the open market.

We further distinguish fictitious pickups from scams in which cargo is not stolen but monies are taken from shippers, freight brokers, and legitimate carriers: for example, expense advances for cargo about to be shipped or in transit.

Our available data comes from incidents of fictitious pickup in which cargo has been lost and reported after the fact. Because victims are often reluctant to report fictitious pickups because they failed to vet carriers and drivers properly, this crime is underreported. However, it now accounts for 8 percent of the reported types of cargo theft (after stolen trailers) and is becoming increasingly more common.¹

WHAT IS FICTITIOUS PICKUP?

Fictitious pickup is a form of cargo theft that involves criminals posing as legitimate truck drivers to steal cargo directly from shippers, sometimes setting up fake transportation companies to do so. It is one of several types of identity theft crimes targeting the motor freight industry that include theft of advance freight payments by commercial wire transfer fraud (T-Chek, Comcheck, and so forth).²

In a fictitious pickup, criminals fool companies into willingly turning over loads to them. They use online load-posting sites to win transportation bids or simply show up as drivers with false credentials, claiming to be assigned to a load. Variations of this scam include a recently terminated driver arriving in advance of his former employer’s assigned driver.³

The Internet has increased the ease with which criminals can set up fake companies and acquire motor truck cargo insurance, and fictitious pickup schemes are proliferating.
FICTITIOUS PICKUP DATA

- Of 1,192 cargo theft incidents reported to CargoNet in 2012, 74 were described as fictitious pickups, a 25 percent increase over 2011. Fictitious pickups are already up more than 8 percent through August 31, 2013.

- The commodities most frequently targeted for fictitious pickups are foods and beverages, electronics products, and metals.

- More than half of fictitious pickups occur at the end of the week, on Thursdays and Fridays, when the main concern of shippers and brokers is to meet delivery dates and satisfy customers. This urgency to deliver causes some shippers, brokers, and warehouse operators to slack off on driver and carrier screening and the due diligence processes to verify IDs.

- Fifty-five percent of all reported fictitious pickups from 2011 through 2013 occurred in California. Significant fictitious pickup activity has also been reported in Florida, Texas, and New Jersey. Interestingly, in some areas of the Midwest — including Indiana, Nebraska, and Wisconsin — conventional cargo theft is relatively rare, but fictitious pickup is occurring.

- The average value of cargo stolen by fictitious pickup was $203,744 versus $174,380 per incident for cargo thefts overall during the study period, a 17 percent differential. This may reflect the fact that fictitious pickups are typically more premeditated, targeted, and carefully planned than opportunistic trailer and container snatches, which constitute the majority of cargo thefts.

<table>
<thead>
<tr>
<th>Day of Week</th>
<th>2011</th>
<th>2012</th>
<th>2013 YTD</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday</td>
<td>13</td>
<td>23</td>
<td>15</td>
<td>51</td>
</tr>
<tr>
<td>Thursday</td>
<td>14</td>
<td>23</td>
<td>9</td>
<td>46</td>
</tr>
<tr>
<td>Tuesday</td>
<td>8</td>
<td>9</td>
<td>14</td>
<td>31</td>
</tr>
<tr>
<td>Wednesday</td>
<td>16</td>
<td>6</td>
<td>4</td>
<td>26</td>
</tr>
<tr>
<td>Monday</td>
<td>4</td>
<td>7</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>Saturday</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>13</td>
</tr>
<tr>
<td>Sunday</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total FPUs</td>
<td>59</td>
<td>74</td>
<td>51</td>
<td>184</td>
</tr>
<tr>
<td>Total Thefts</td>
<td>1201</td>
<td>1195</td>
<td>605</td>
<td>3001</td>
</tr>
<tr>
<td>FPU %</td>
<td>5%</td>
<td>6%</td>
<td>8%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Table 1: Fictitious Pickups 2011–2013 YTD (Incidents reported to CargoNet)
Chart 1: Fictitious Pickups as a Percentage of Total Reported Cargo Theft (Incidents reported to CargoNet)

Chart 2: Fictitious Pickups by Commodity Type (Incidents reported to CargoNet)
There appears to be a strong correlation between commodities targeted for fictitious pickups and overall cargo theft. Foods and beverages, electronics, and metals are most attractive, though fictitious pickups of metals have declined in 2013, possibly because of new security regulations.
Approximately 35 percent of all cargo thefts occur on Saturdays and Sundays versus only 8 percent of fictitious pickups. More than 50 percent of fictitious pickups occur on Thursdays and Fridays, when shippers and warehouses are busiest.

California, long a hotbed of conventional cargo theft, has become the top U.S. fictitious pickup state.

*Note: The data in the above charts is based on incidents reported to CargoNet. While reporting continues to improve, these numbers do not represent the true totals of cargo theft or fictitious pickup incidents.*

**FICTITIOUS PICKUP: HISTORY**

Historically, freight brokers are trusting; they’ll readily turn over a trailer with $1 million of tablet computers to someone they’ve never met. Before the advent of the Internet and the growth in non-asset-based logistics providers and freight brokers, transportation arrangements were based on long-standing relationships and made with face-to-face trip lease contracts. Since motor freight carriers and drivers were familiar to brokers, identity verification was perfunctory or nonexistent.

Fictitious motor freight pickups began to emerge as a trend around 2005. The crime has grown since then, and 2011 saw a marked increase in fictitious pickups. The California Highway Patrol’s Cargo Theft Interdiction Program (CTIP) reported “significant increases in reported fraud and company identity theft loads with fifty-one (51) loads in 2011 compared to five loads (5) in 2010.”

Fictitious pickups have grown alongside the expansion of web-based brokering, the ability to set up fictitious companies and websites, and the availability of high-quality fraudulent driver’s licenses. The Just In Time (JIT) supply chain management practices have exacerbated the problem by putting a premium on speed at the expense of performing time-consuming due diligence in vetting...
CargoNet predicts that computer-savvy criminals (often former employees of trucking and logistics companies) will increasingly turn to this modus operandi because it is less risky than traditional cargo theft.

Criminals can avoid being tracked by using prepaid cell phones and cloaking financial transactions with branded, prepaid credit cards. With these prepaid services, there is no way to trace the payment and determine the identity of the user.

**HOW DOES A TYPICAL FICTITIOUS PICKUP SCAM WORK?**

It is easy to set up a fictitious logistics company by using prepaid credit cards, operating out of a P.O. box, and even obtaining a Federal Tax Identification Number or EIN (Employer Identification Number). Shell companies can register a name with the Department of Transportation, obtain an Interstate Operating Authority Number (MC, or Motor Carrier, Number), and even get cargo and liability insurance over the Internet. A rented or stolen tractor can be cloaked with temporary company placards, and the driver can obtain and wear a fake “company” uniform.

Misspelling of “Truking” is a tip-off that the operation is fake.
This adhesive placard was found on the door of a stolen tractor.

Criminals search online load boards for commodities that are easy to fence. Late Friday afternoon pickups are preferred, when shippers are anxious to move product out and less rigorous with driver vetting. The drivers arrive with fake IDs and masked trucks, tender their paperwork, load, and depart. After one or two calls to assure the shipper or broker that drivers are en route, the criminals are never heard from again.

**SEVEN BEST PRACTICES TO PREVENT FICTITIOUS PICKUP**

The keys to preventing fictitious pickups are common sense along with a connected, information-enabled, collaborative supply chain that responds quickly and decisively to external threats.
1. Situational Awareness
Subscribe to CargoNet and SC-ISAC for daily reports of fictitious activity in your area and region. And if you are ever a victim, quickly report incidents and attempts to law enforcement and CargoNet.

Identity Theft

Incident Description
On 5/30/2013 at 11:49 p.m., ABC Express Logistics received a call from a man with an Eastern European accent claiming to be Charles of Transportation Enterprises. The suspect was interested in a commodity of bottled juices going from Los Angeles to Atlanta, GA, and then Florida. The carrier wasn’t yet set up with ABC, and ABC e-mailed their packet to him. He offered to do the job for $6,000, which was a red flag to the company. They checked SAFER and realized his information did not match. They requested that he call back with the SAFER information. The man never called back.

ABC called the legitimate owner of Transportation Enterprises, James Smith, and he said that he had never heard of a Charles or the number Charles called from. The suspect is using Transportation Enterprises’ identity and now may try to use ABC Express Logistics’ identity, too. The legitimate information for ABC Express Logistics and Transportation Enterprises is included below.

Legitimate Company Information
Company Name: Transportation Enterprises
Address: 123 Main Street, Herndon, VA 24251
USDOT Number: 12345678
MC Number: 987654
Phone: 123-555-8795 (This number is different from SAFER, but that number is dead, and the owner of the company said this is the new number.)

Company Name: ABC Express Logistics LLC
Physical Address: 4100 125th St, Akron, OH 12345
Mailing Address: 4545 Senator St., Akron, OH 45242
USDOT Number: 8585858
MC Number: 3648752
Phone: 987-654-3211

Suspect Information
E-mail address used: TransportationEnterprises@yahoo.com
Name used: Charles (driver/dispatcher)
Phone used: 675-246-6312
Eastern European accent

Contact Information
Those with information are asked to contact the CargoNet Command Center at 1-888-595-2638.

Disclaimer:
The following report does not reflect the opinions of CargoNet and the Transportation Intermediaries Association (TIA). We neither encourage nor discourage anyone from conducting business with any company. Please use your own independent judgment when making such decisions.

To learn more about CargoNet or to become a member, please call 1-888-595-2638 or e-mail info@cargonet.com. You may also visit us online at http://www.cargonet.com/.
2. Supply Chain Collaboration
Collaboration and frequent, timely communications among shippers, carriers, brokers, and consignees are essential to a secure supply chain. The first and foremost element in a secure supply chain protocol is validation, especially of third parties. When booking loads from a broker, confirm all company information before scheduling a shipment. Call and verify that the broker is legitimate.

3. Secure Chain of Custody
Know where your cargo is — and who has it — at all times. Ensure an unbroken chain of custody to prevent fictitious pickups, and take advantage of intelligent routing, shipper/carrier communications protocols, telematics, real-time monitoring, GPS tracking, and geo-fencing technologies.

4. Carrier Security Protocols and Communications
Carriers must agree to adhere to all of the shipper’s security guidelines and assume responsibility for the full value of lost, damaged, or stolen goods if proven noncompliant. Tractors and trailers must both be equipped with an active GPS tracking system. For each load tendered, the carrier must provide in advance the driver name and photo, tractor and trailer numbers, and unique appointment or cargo release numbers. Frequent (every four hours) status updates must be provided by cell phone, and vehicle location should be actively monitored by GPS.

5. Carrier Vetting
Know who is carrying your cargo. Begin by performing a Dun & Bradstreet check on company history, including years in service and financial condition. Verify references. FMSCA’s SAFER (Safety and Fitness Electronic Records) system provides company snapshots by USDOT and MC/MX numbers and company name: [http://safer.fmcsa.dot.gov/CompanySnapshot.aspx](http://safer.fmcsa.dot.gov/CompanySnapshot.aspx). Validate insurance information by calling the insurance company and cross-referencing company contact information and phone numbers. Inspect ACORD forms to ensure all information is consistent. Search for the company’s website; it is a big red flag if you cannot find it or the information does not match up. Confirm that the company has a land-line telephone. Be sure e-mail addresses match the carrier’s domain name exactly. Be wary of carriers responding to load postings on the Internet. Avoid brokering high-value, high-risk loads; the cost savings are not worth the risk. If the carrier’s address is a P.O. box, be wary. If there is a street address, use GIS mapping tools such as Google Earth or MapQuest with satellite views to verify the company is located at a commercial site.

6. Driver Vetting
Evaluate risk and reduce liability by screening job applicants as well as current employees, including accessing their Driving History Reports. Consider using a service that continuously monitors for changes to MVRs, such as iIX’s ExpressNet DriverSafe® and DriverAdvisor® monitoring. [http://www.iix.com/monitoring.htm](http://www.iix.com/monitoring.htm)
Falsified license with two people in the driver photograph. This time the evidence was plain.

7. Secure Cargo Release Process
Carefully inspect at least two forms of identification, including government-issued and company IDs. Use a driver’s license scanner to authenticate commercial driver’s licenses (CDLs). Ask to see the driver’s US DOT Medical Examiner’s Certificate; all drivers are required to have one, but no one thinks of asking for it.

Take a close-up photo of the driver, making sure the face is clearly visible and unobstructed. Capture biometric information — a fingerprint is ideal — digitally, if possible. Take a high-definition photo of all IDs; photocopies often miss important details. Requesting this is an effective deterrent; drivers with bad intent will often return to their trucks to get additional information, never to be seen again. This information is tremendously helpful to law enforcement in investigating and prosecuting crimes.

Query the diver for the appointment or cargo release number that was provided to the carrier, and compare for a match. Check documentation — Bills of Lading, Air Waybills, and so forth — for accuracy and obvious errors, and require the driver to sign and print his name on it, comparing the signature to the CDL. Make scanned images of the shipping documents tendered to be associated with driver and carrier information. Carefully inspect the truck, making note of tags and ID numbers while looking for obvious discrepancies, evidence of ghost and/or temporary signage, or recent attempts to conceal trailer markings. Capture photos and/or digital video images of the truck, license plates, and the like.

If the driver appears nervous, double-check everything. In addition, check online watch lists for terminated employees and known criminals.
A NOTE ABOUT PROTECTING DRIVER PRIVACY

Protecting a driver’s personal information during ID validation is a legitimate and serious concern. It is therefore essential that all personal information collected be securely handled and stored.

Driver Identification, Registration, and License Validation Tips

• ID Verify is an online, web-based system for validating the identity of drivers and personnel transporting cargo. https://www.securecargo.org/products/id-verify-system
• A specialized visitor management system, such as Regiscope’s Cargo Cam, specifically designed for cargo shipping and receiving facilities, registers all drivers picking up and delivering cargo to and from the facility and validates their licenses (CDLs): http://www.regiscope.com/content/cargo-cam-0. The Cargo Cam system captures digital photographic and video images of drivers and vehicles, digital fingerprints, and scanned images of the documentation tendered with cargo (Bills of Lading, Air Waybills, and so forth).
• As fake licenses become harder to detect, an online authentication service should be used. This service asks drivers a series of questions to which only they will know the answers. http://www.idology.com/knowledge-based-authentication/dynamic-kba

THE BROADER IMPACT OF FICTIONAL PICKUPS

Cargo theft can have a much bigger impact than the cost of a lost load, truck, or trailer. Other costs include the time and effort involved in recovery operations and replacing and restocking lost inventory. There is also the potential for disruption of your customer’s operations and the loss of future business from those who count on reliable deliveries. In cases where pharmaceuticals, foods, beverages, or other regulated or dangerous products are involved, recalls and public relations may further add to the cost of cargo theft — and public safety can be at risk.

SUMMARY

Fictitious pickups are a growing threat to the safety and security of the supply chain, especially to the motor freight industry. The strongest deterrent is better information that can be shared rapidly and accurately among supply chain trading partners and carriers to prevent this crime. In conclusion, to prevent fictitious pickups, one must fight information with information. We urge concerned shippers, 3PLs, brokers, and motor freight carriers to implement rigorous carrier and driver vetting procedures and to invest in, and become proficient in the use of, the well-proven and readily available information technologies that can successfully combat this growing threat.
NOTATIONS

1. CargoNet, CargoNet database and application
2. T-Chek’s Express Cash™ and Comchecks are payment instruments given by companies to be used by drivers as an advance for trip expenses, including fuel, which can be issued in amounts well over $1,000 for long-haul trips. In a Comcheck scam, a load is found on an Internet posting board and booked with a 3PL using prepaid cell phones, one with the area code set from the carrier’s location, the other from the “shipper’s” location. The “shipper’s” phone is used to call the 3PL to notify the carrier that the load has been “picked up.” The Comcheck is secured, and the phones are dumped.
6. A standard Trip Lease Agreement is used for a single trip or a lease of short duration. This agreement is a preprinted form on which the required information is entered. It also has provisions for designating the exact time the lessee took possession of the equipment and the exact time the lessee released the equipment.
8. Credit to S/A Tom Vagasky, Illinois State Police

SOURCES

2. Supply Chain Information Sharing and Analysis Center (SC ISAC), SC ISAC Operations Center https://secure.sc-investigate.net/SC-ISAC/ISACMemberHome.aspx
ABOUT CARGONET

A division of the Verisk Crime Analytics unit at Verisk Analytics (Nasdaq:VRSK), CargoNet® helps prevent cargo theft and improve recovery rates through secure information sharing among theft victims, their business partners, and law enforcement. CargoNet is centered on a national database and information sharing system managed by crime analysts and subject matter experts. By applying a synchronized, layered approach, CargoNet exploits the weaknesses of cargo thieves at multiple points. CargoNet offers integrated databases, a theft alert system, task force and investigations support, and a tractor/trailer theft deterrence program. CargoNet also provides driver education and incentives, secondary market monitoring and interdictions, crime trend analysis and loss control services, and training. More information on CargoNet can be found at www.cargonet.com.

ABOUT THE CARGO SECURITY ALLIANCE

“Secure the global supply chain; expedite the flow of commerce.” The Cargo Security Alliance (CSA) provides tools, techniques, technologies, and thought leadership in logistics security to mitigate risk and optimize cargo flow across the global air, sea, and land supply chains. CSA offers its clients best practices solutions that meet or exceed U.S. and international regulatory standards while delivering operational efficiencies, increased customer service levels, and other benefits that more than offset the costs of added security measures.