



RunBuggy

Transport Security in the Repo Community

October 2025

Agenda

Who is RunBuggy?

Security and Theft: What We are Seeing in Transport

Virtual & Physical Vulnerabilities

Lender Expectations As We See Them

What Stakeholders Can Do. What Agents Should Do

Q & A

Who Are We?



Max Graupner | SVP Security & Audit



For more information, please contact

Jason Kong | SVP Operations
Jason.Kong@RunBuggy.com

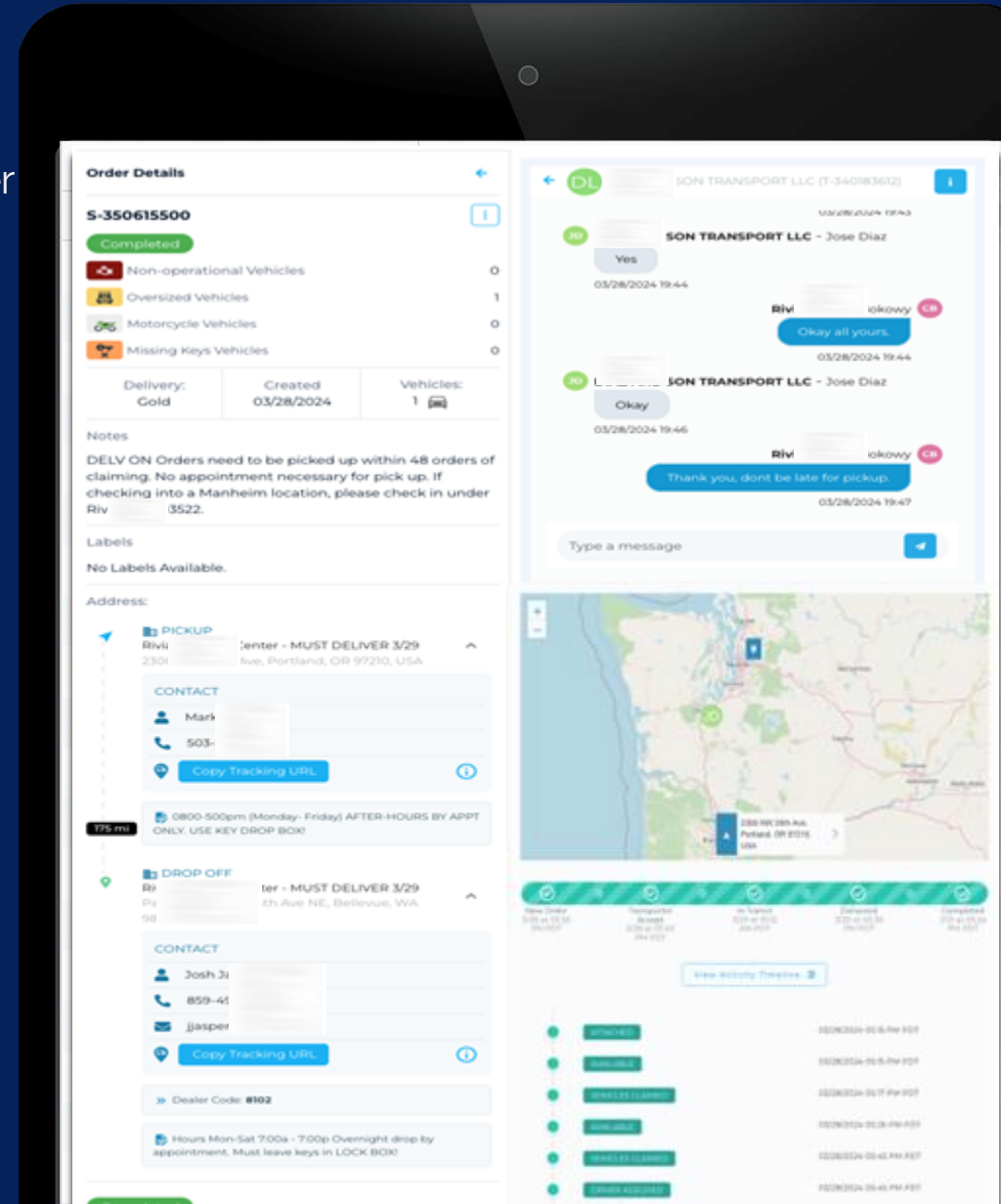
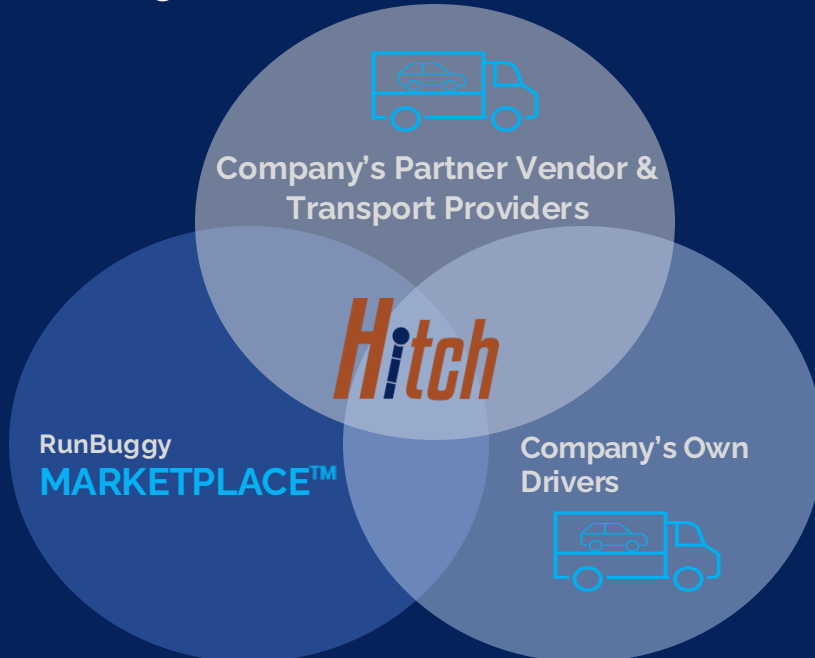


Olianna Dean | Snr Dir of Delivery Ops

RunBuggy is a technology company that connects car shippers and transporters, integrating transportation into your tech stack.

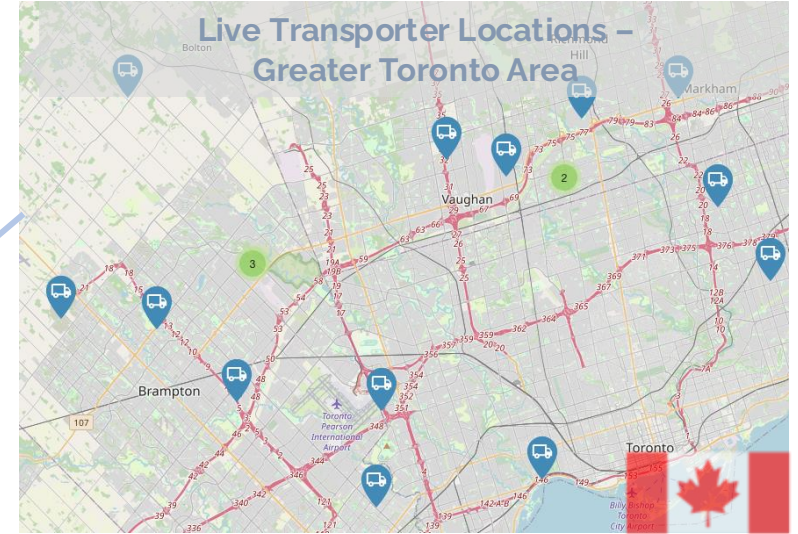
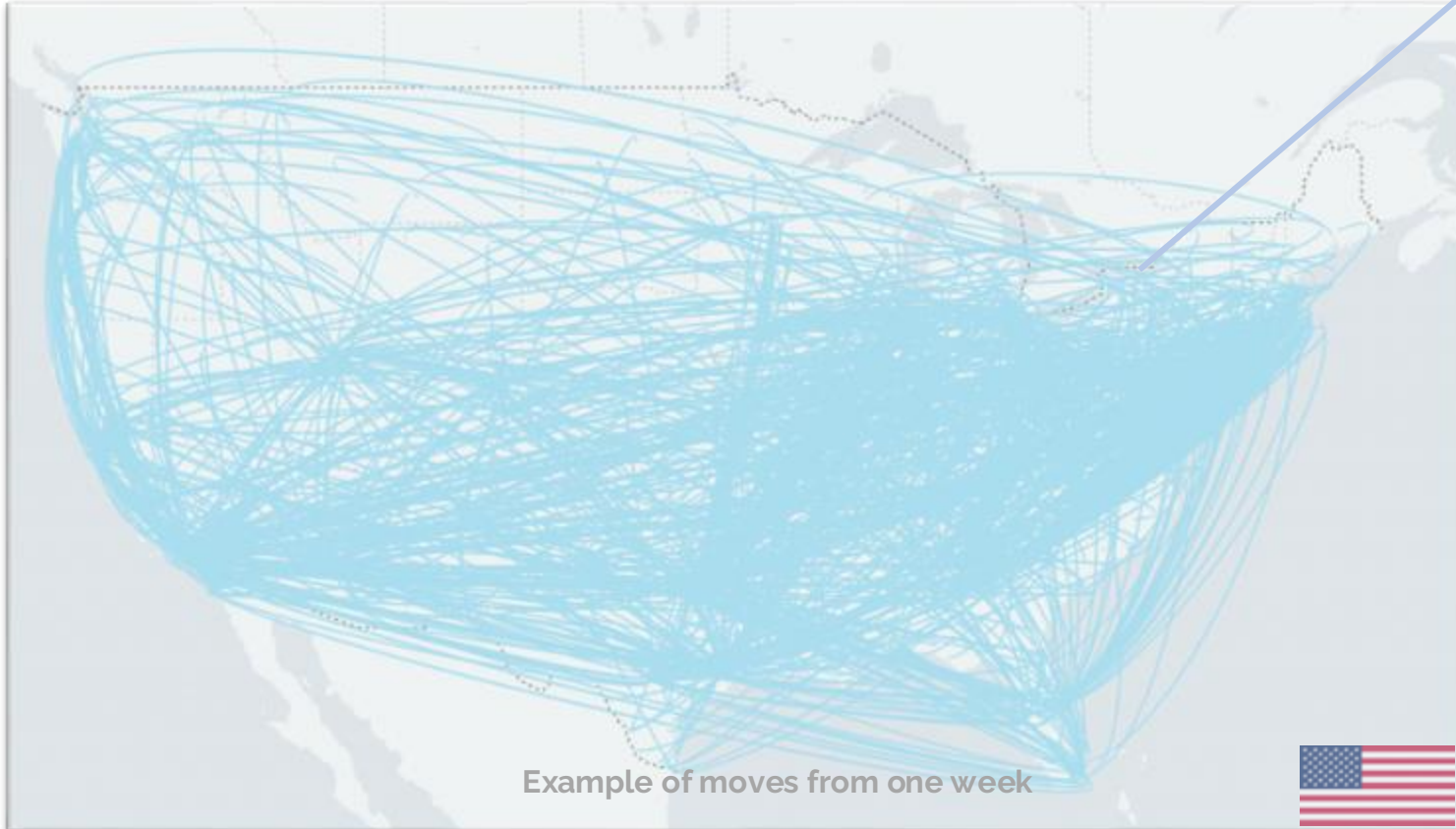
RunBuggy **MARKETPLACE™** is a Transportation-as-a-Service solution using a **moderated, cloud-based logistics** platform and **best-in-class customer service** to help delivery cars faster, at less cost, and with greater efficiency than ever before.

RunBuggy **HITCH™** is a SaaS solution that connects a company's own Drivers, **Partner** Transporters and Vendors with the RunBuggy **MARKETPLACE™**, providing a single secure command center for all transportation management.



International Network

Instant Supply Chain Resilience
17,000+ Drivers Onboarded U.S. + Canada



Every Use Case

Any Point to Any Point. Across the Country.

Full Loads
Partial Loads
Routine Moves
Deviations
Dealer to Dealer
Consumer Direct Deliveries or Pickups
Enclosed
High End / Unique
Remarketing / Repo to Auction
Inoperable Vehicles
Omnichannel Retailing
... And More.



----- Security and Theft: The Problem

[HOME](#) [REPO AGENT SEARCH](#) [CUCOLLECTOR](#) [NEWS](#) [CURREPOSSESSION STORE](#) [PRESS](#)

Home / Press Releases / ARA Alert – Transporter Fraud

ARA Alert – Transporter Fraud

Of Note - July 24, 2025

The graphic features the ARA logo (American Recovery Association) in the top left corner. The main text 'ARA Alert – Transporter Fraud' is written in a large, bold, italicized font with a red-to-white gradient. The background of the graphic shows a black and white photograph of a car being loaded onto a transport trailer by a crane.

Thieves Hacking Transport Brokers to Steal Repossessions

ARA Members,

Over the past several weeks, ARA has received troubling reports that a dangerous trend long affecting the auto dealer world is now making its way into the repossession space, and it's putting our members at serious risk.

Here's what's happening:

A client, let's call them Not Named Financial, sends a release order to an auction. That auction, in turn, uses a broker to locate a transporter to retrieve the vehicle. Somewhere in this chain, the release order is intercepted or manipulated, and a transporter shows up to your lot with seemingly legitimate documentation. You follow protocol, verify the paperwork, and release the unit.

The problem? That transporter isn't who they say they are, and the vehicle is never seen again.

This isn't a hypothetical. It's happening. And if you're thinking, "Well, I followed instructions and verified the release," that's exactly the issue – the agent did everything right but still is held accountable for the loss. In the eyes of the client or insurer, that vehicle is now "stolen."

Microsoft

Security and Theft: The Problem



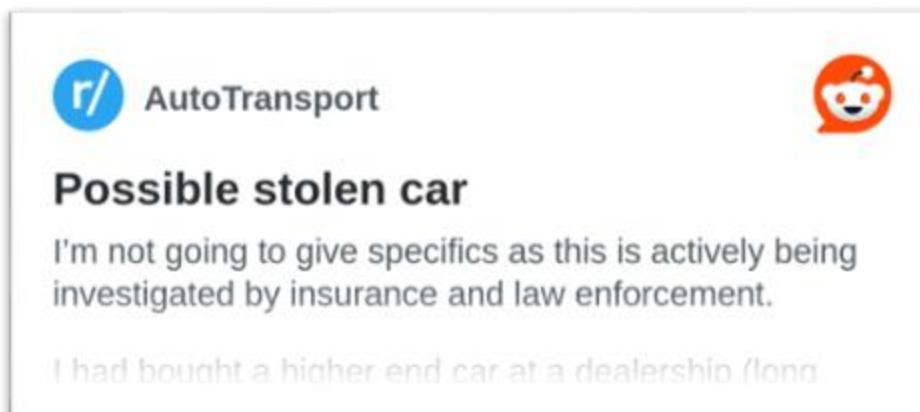
Clients who allow agents to coordinate 100% of their transport directly,

*Somewhere in this chain, the release order is intercepted or manipulated, and a transporter shows up to your lot with **seemingly legitimate documentation***

1. **Vet every transporter** thoroughly. If it didn't come from the client or auction directly, question it.
2. **Document** everything. Who sent the release? Who's picking up? Who **confirmed** the transport?
3. Have the transport companies send valid workers' compensation insurance certificates from their carrier.
4. Push back. If you're uncomfortable or something doesn't feel right, **stop the release** and get written confirmation from the client
5. **Educate** your clients. Let them know this is happening. Many of them don't realize the risk they're creating.

MUCH Bigger than Repo or Remarketing!

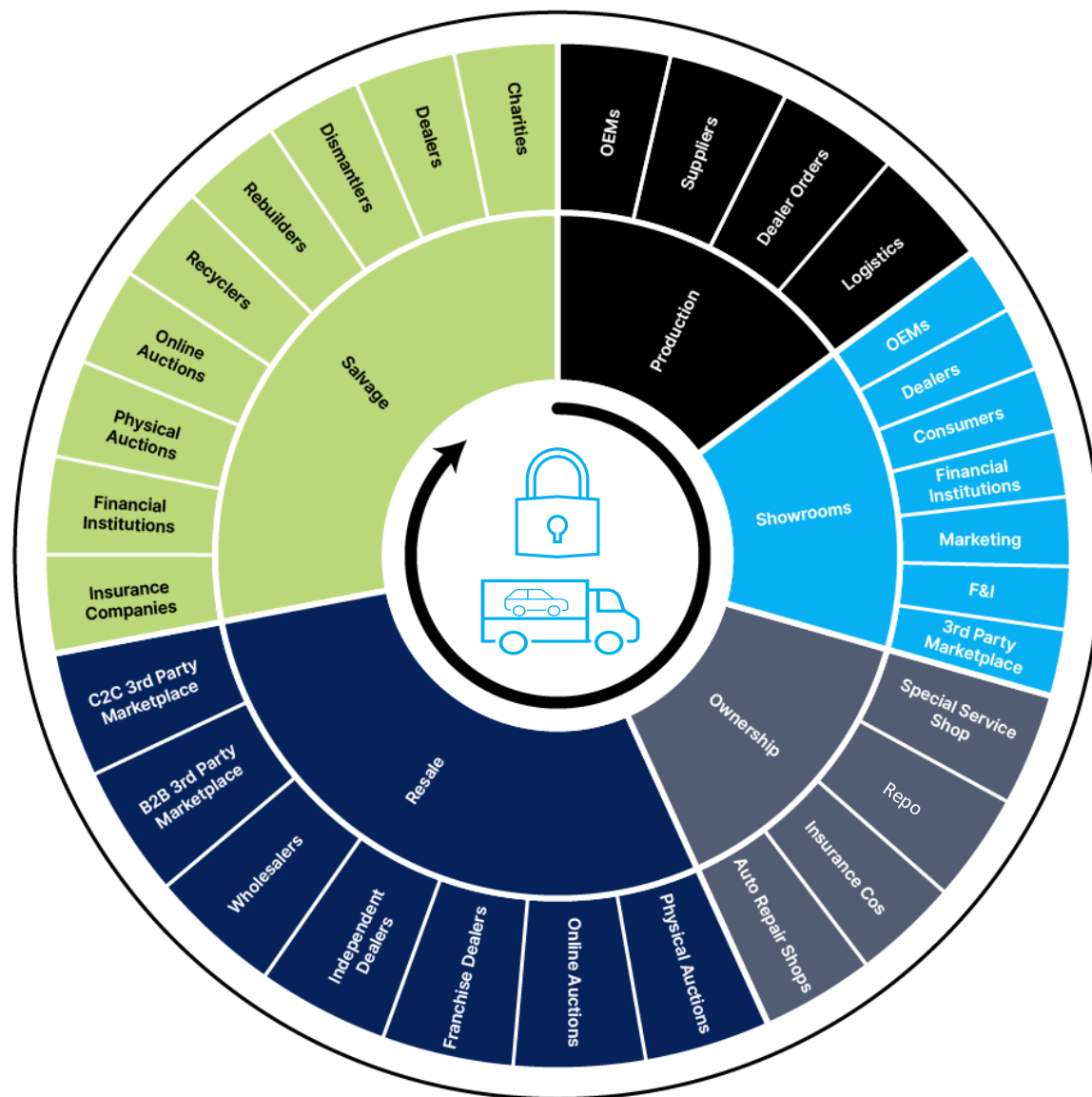
----- Security and Theft: What We Are Seeing In Transport

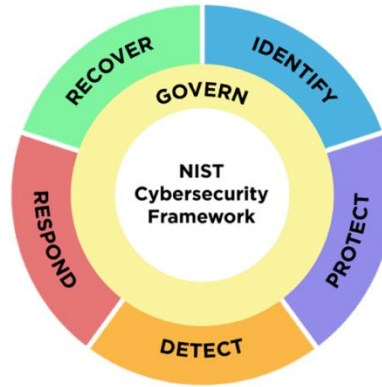


MUCH Bigger than Repo or Remarketing!



How to Protect the Entire Ecosystem

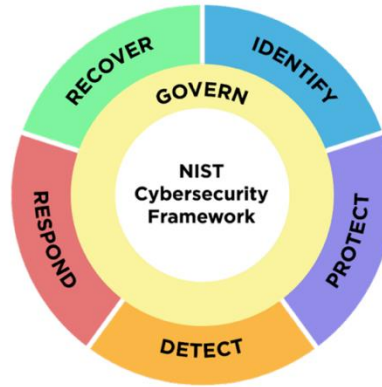




Manage Risk with a Strong Security Posture

*The security status of an enterprise's **networks, information, and systems** based on information security resources (e.g., **people, hardware, software, policies**) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.*

https://csrc.nist.gov/glossary/term/security_posture



Manage Risk with a Strong Security Posture

Improve robustness and resiliency with **overlapping layers and redundancy**

Effective overlap creates a multi-layered defense where different tools can catch threats the other missed, and redundancy ensures continuity by eliminating single points of failure

Professional Criminals

High Dollar Vehicles

Professional Criminals

High Dollar Vehicles



Physical Vulnerabilities



Vulnerabilities in
People, Processes, Policies



Vulnerabilities in
Technology

Professional Criminals

High Dollar Vehicles



Physical Vulnerabilities

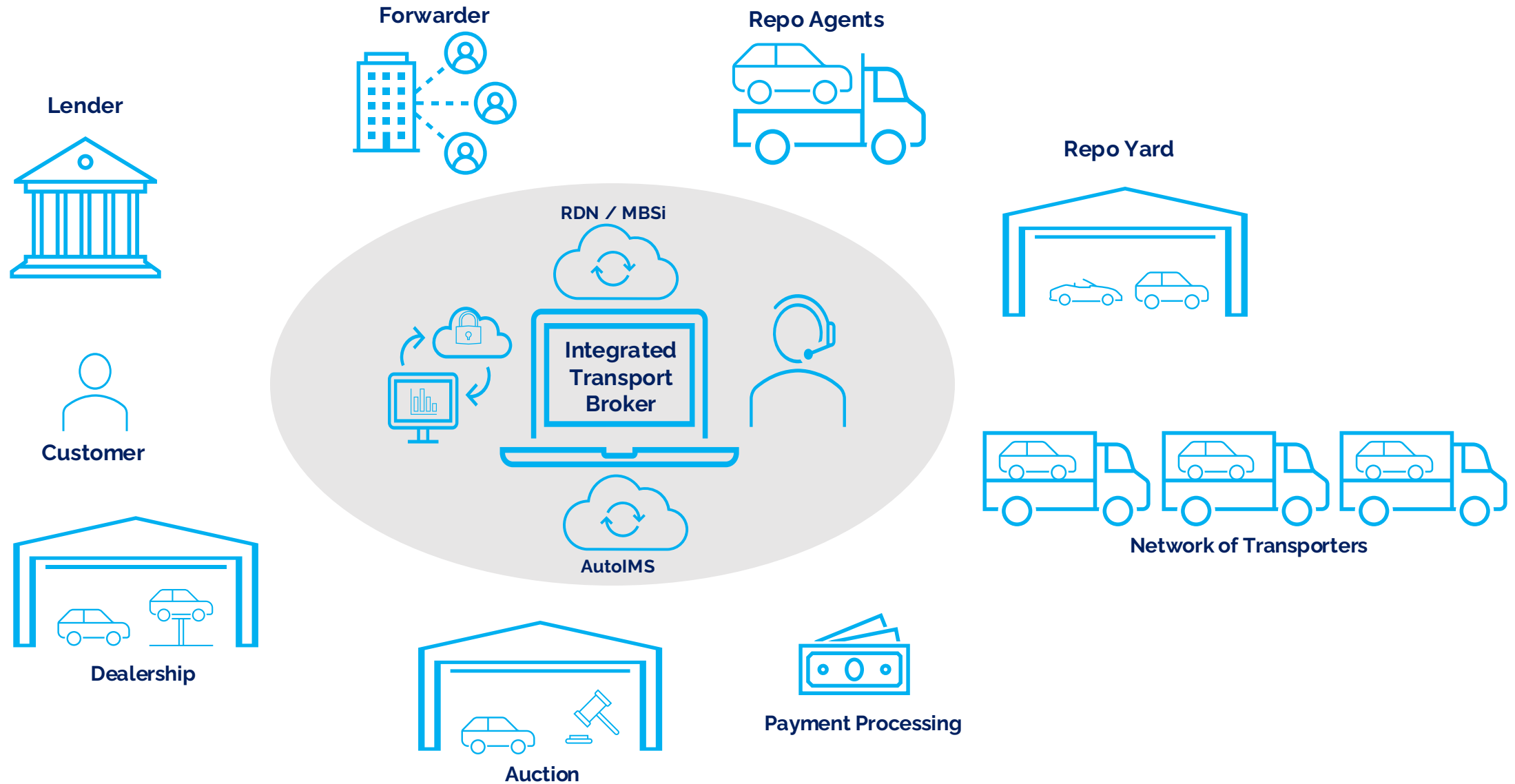


Vulnerabilities in
People, Processes, Policies

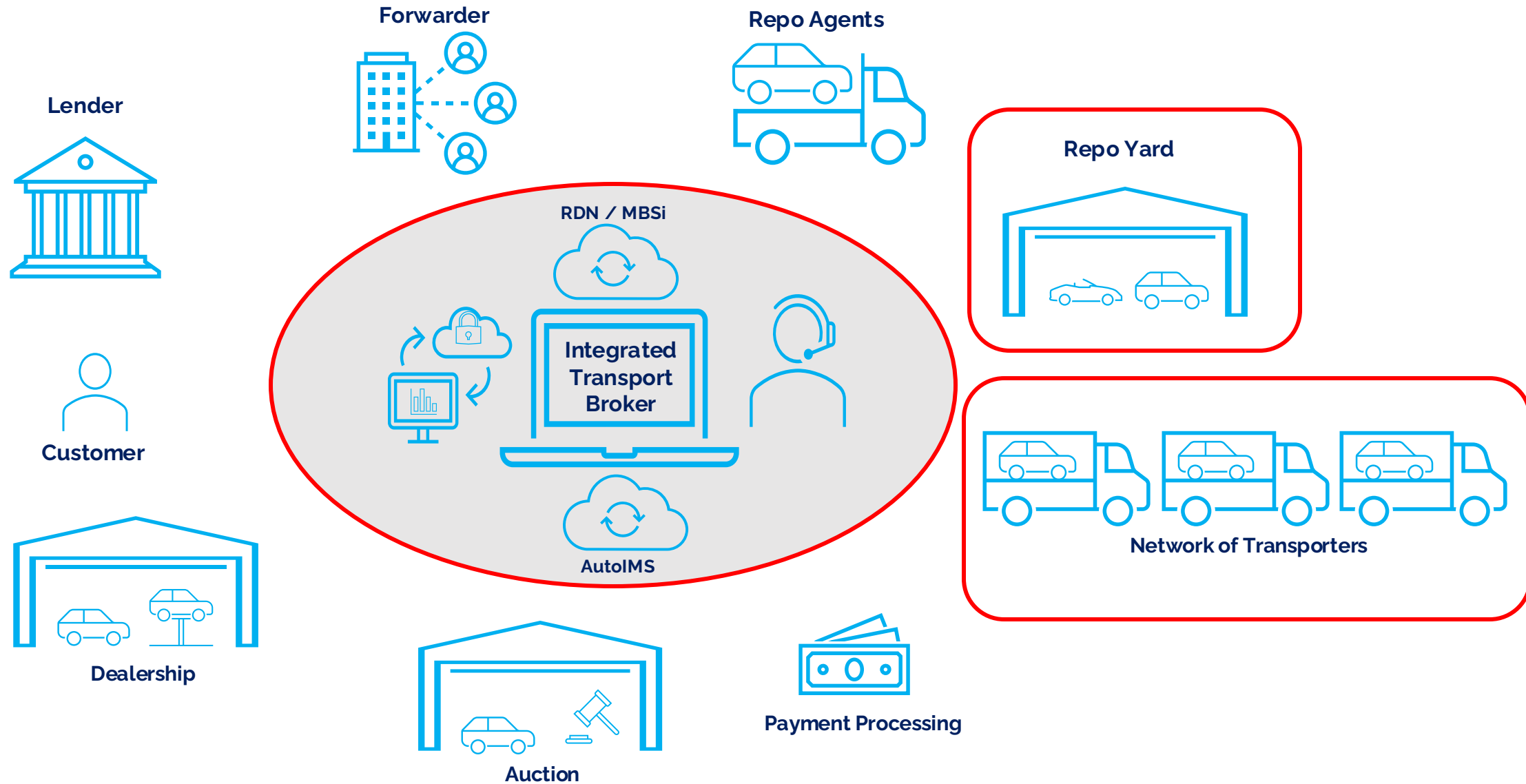


Vulnerabilities in
Technology

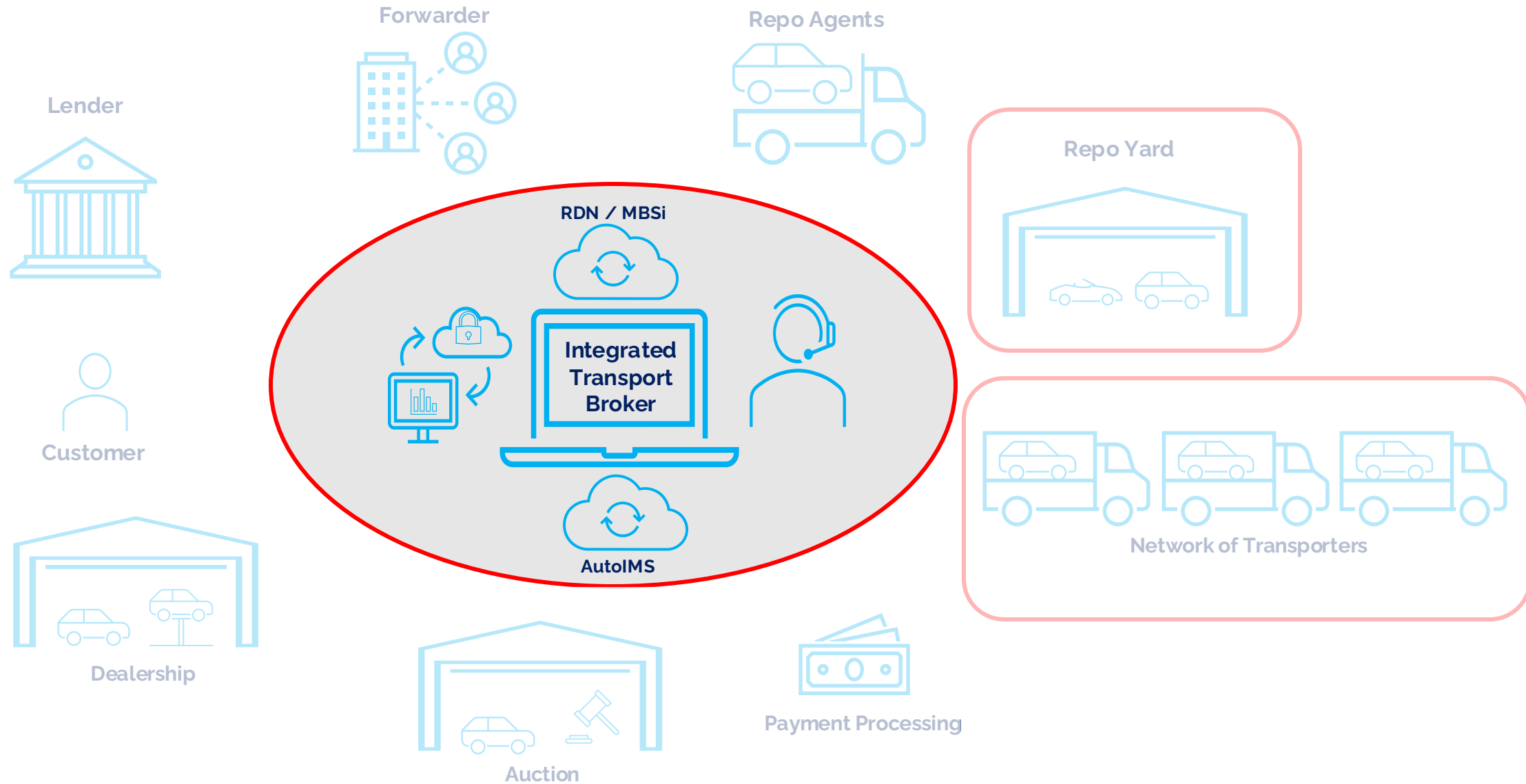
Remarketing Transportation Ecosystem



----- Remarketing Transportation Ecosystem: Focus for Today's Conversation

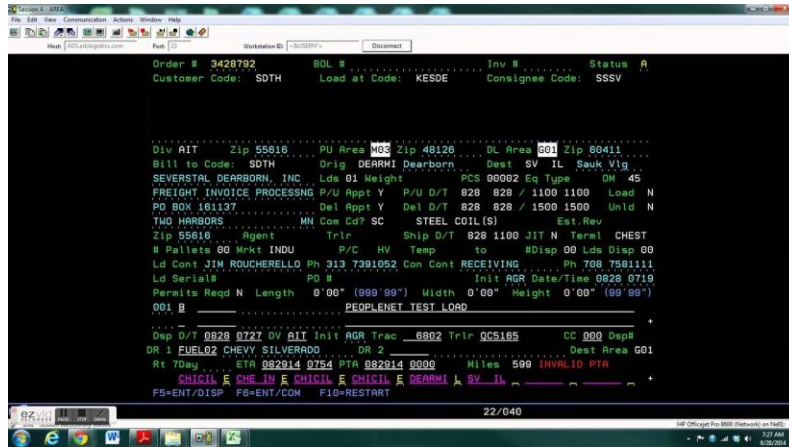


----- Remarketing Transportation Ecosystem



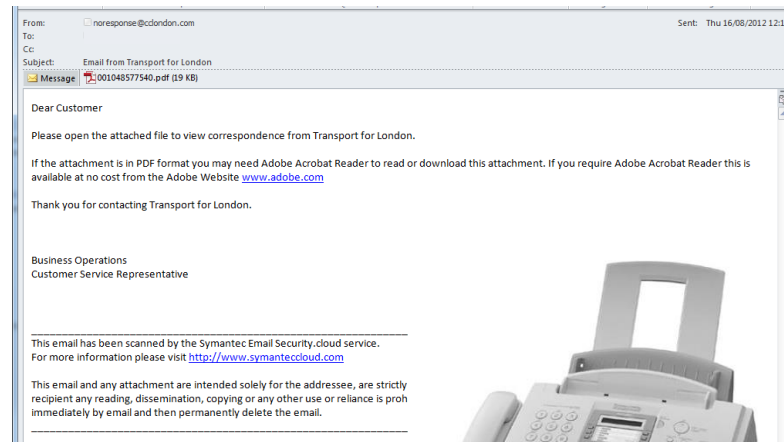
----- Legacy Transportation Data Ecosystem

Standardization for communication is difficult!



Archaic Systems
OEM: AS400

No integrations or commonality



Manual Processes and Communications
One to one communication threads

Email and Fax

Fragmented Data Sources
Inconsistent, primitive, analog

Paper Bills of Lading

Bank-Grade Cybersecurity

Battle-tested, proven cybersecurity protection for every transaction

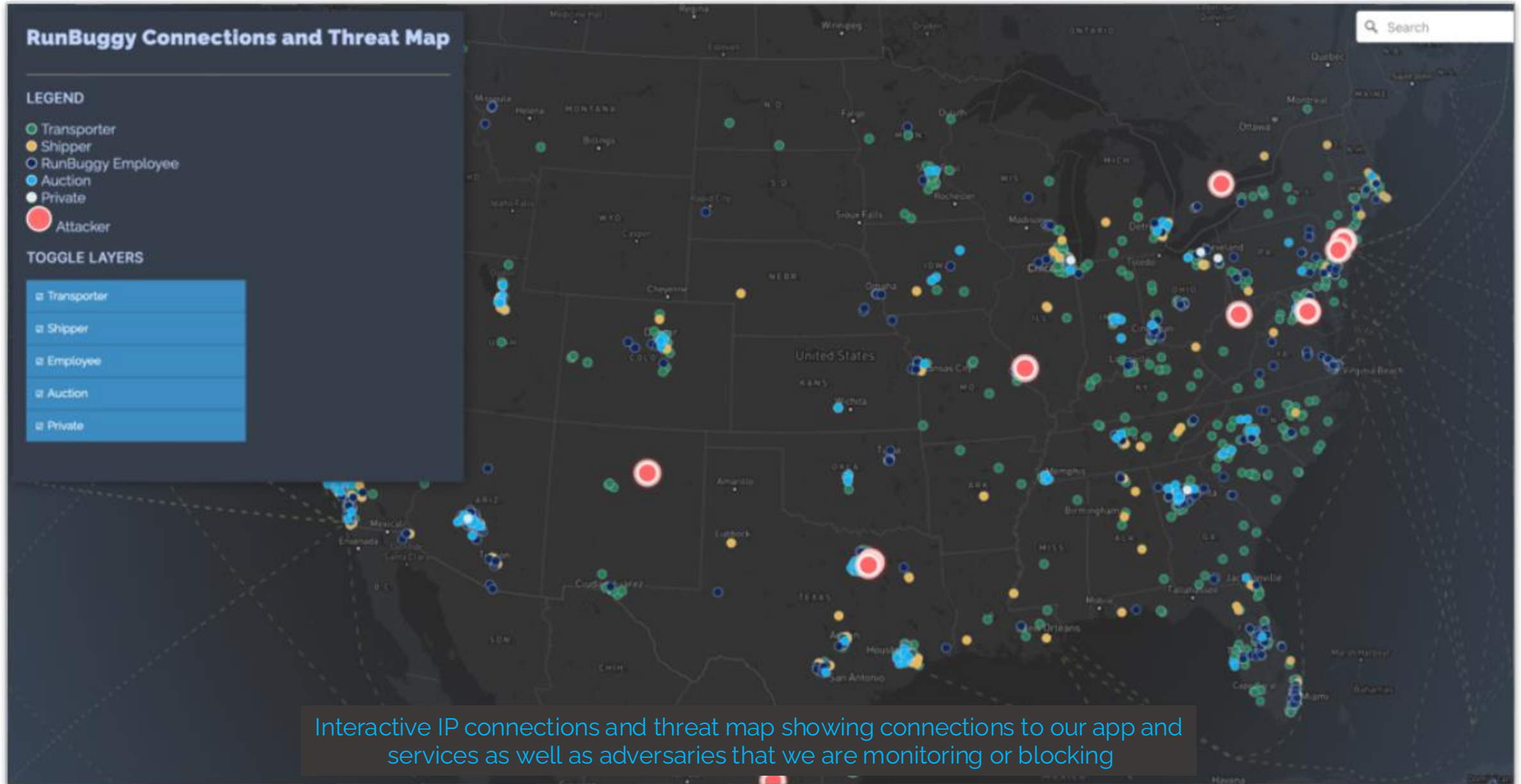
Transportation platforms processes millions of transactions and millions per month in payments from shippers and fares to transporters.

The NIST logo is displayed in white on a dark gray square background.The PCI DSS logo is displayed in white on a dark gray square background.The OWASP logo is displayed in white on a dark gray square background.The SOC 2 Type 2 logo is displayed in white on a dark gray square background.The ISACA logo is displayed in white on a dark gray square background.A stylized white logo resembling a lowercase 'a' or a drop shape is displayed on a dark gray square background.

Global OEMs, Lenders, and Large Enterprise Accounts Require This

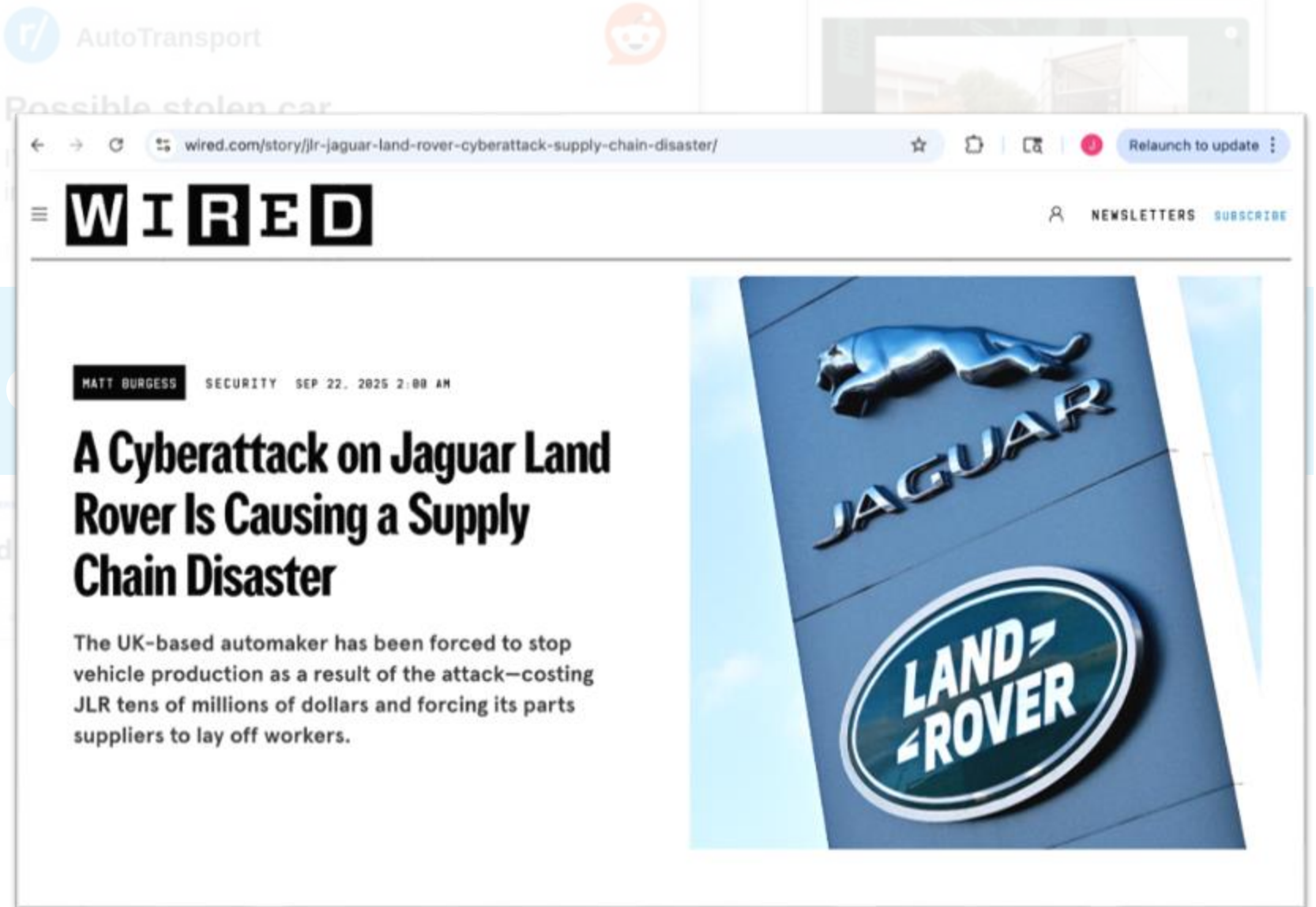
Why?

Professional Bad Guys: Cyber Threats Are Everywhere

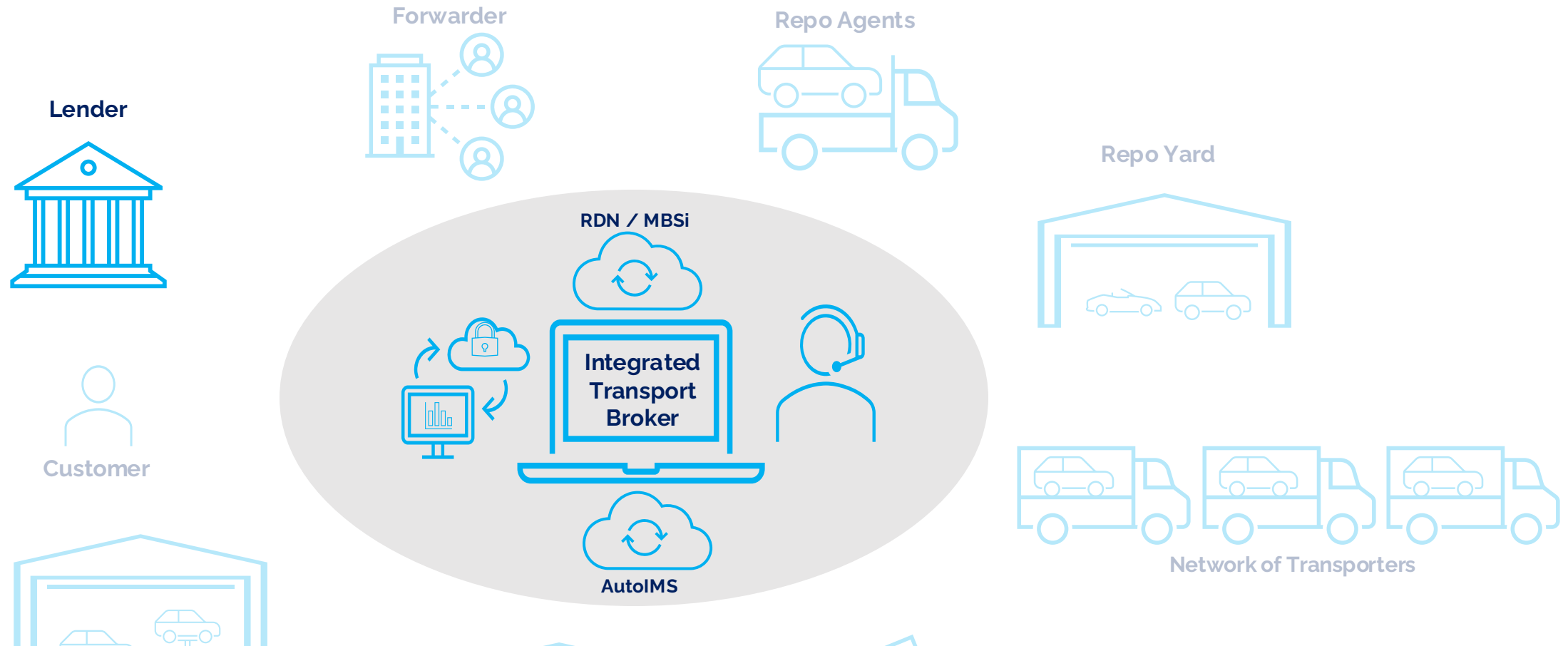


----- Security and Theft: What We Are Seeing In Transport

Procurement and cybersecurity departments are trying to prevent this with **companywide** protections; not limited to vendors of one department

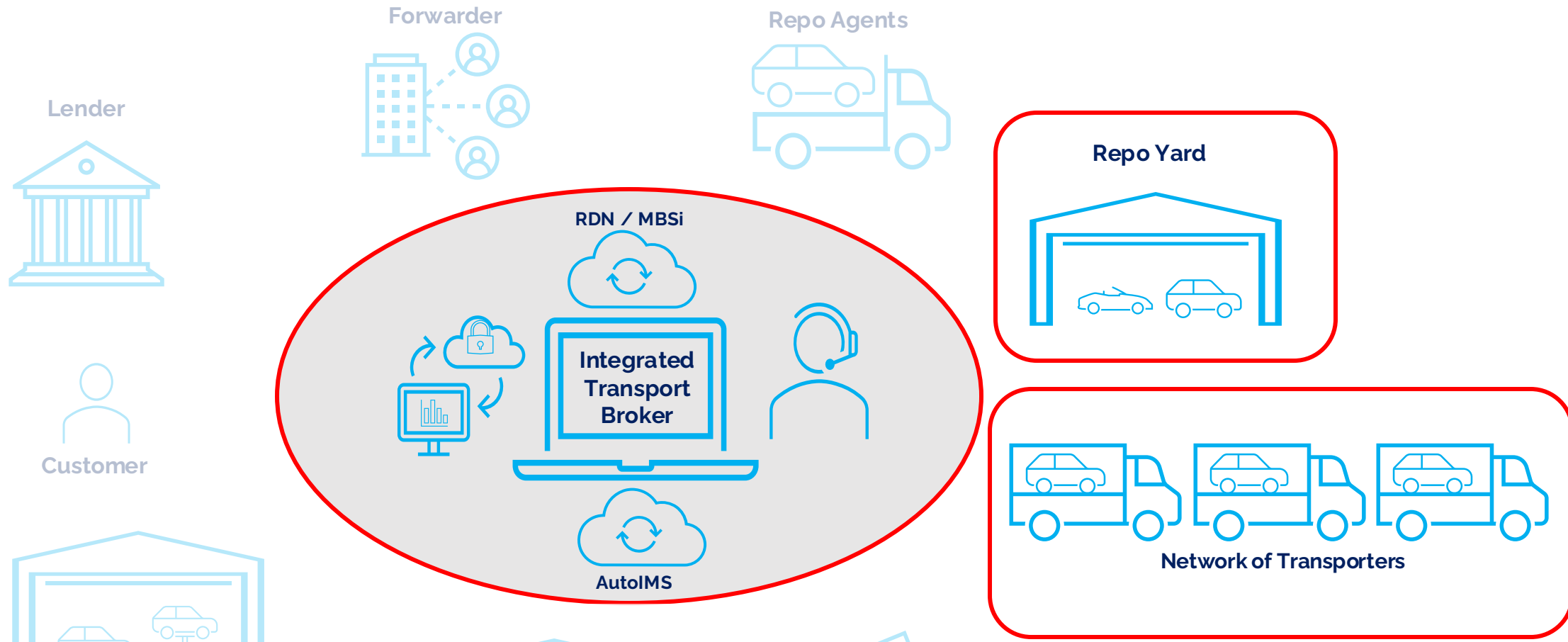


----- Remarketing Transportation Ecosystem



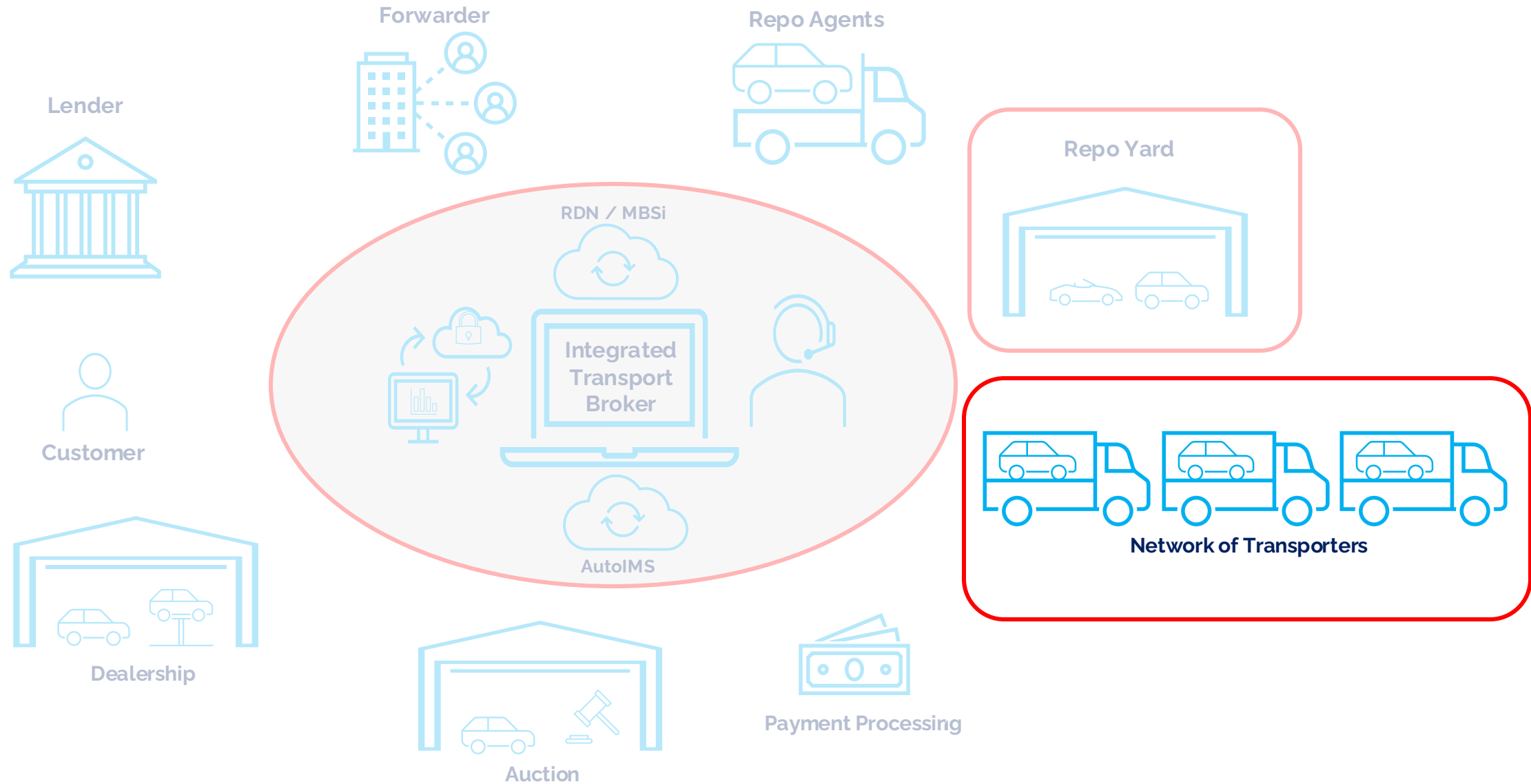
As Long as Enterprise Companies Are Around,
Technology is Not Going Away

----- Remarketing Transportation Ecosystem



Social Engineering, Phishing, Weak Processes

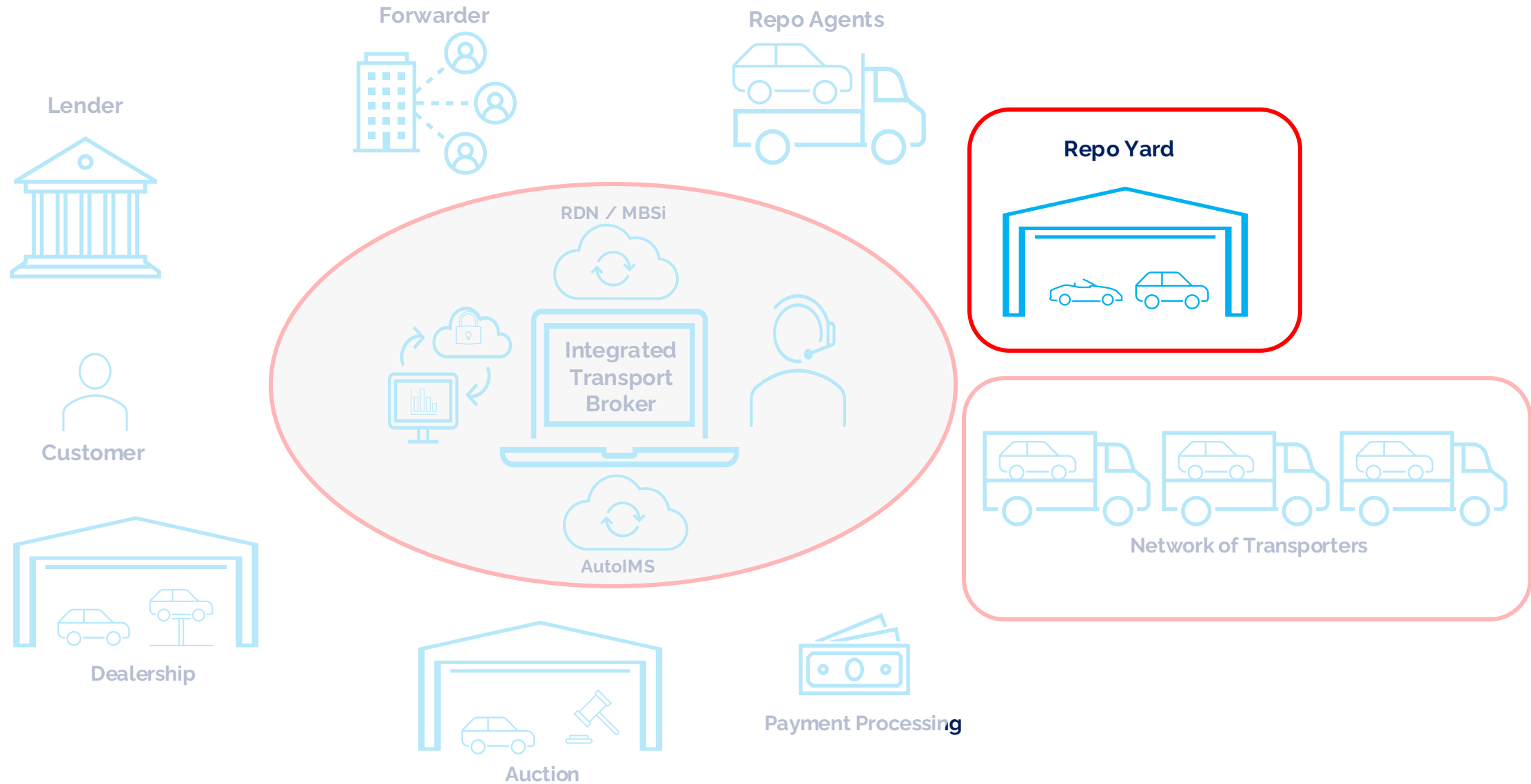
----- Remarketing Transportation Ecosystem



Vulnerabilities in People, Processes, Policies

- Double brokering
- Providing identifying information on load boards
- Not using appropriate processes and authorized systems in place 100% of the time
 1. Bad guys monitoring, probing for weakness
 - Fake or impersonated credentials
 - Sometimes, no impersonation needed; weak processes and key handover at pickup
 - Go pick up vehicle, take where they want
 2. Bad guys intercepting information, setting up innocent transporters to pick up and drop off what they think is a legitimate order
 - Original pick up location
 - NEW drop off location accessible to bad guys
- If the pickup location was not involved in creating the order, they are often clueless

----- Remarketing Transportation Ecosystem

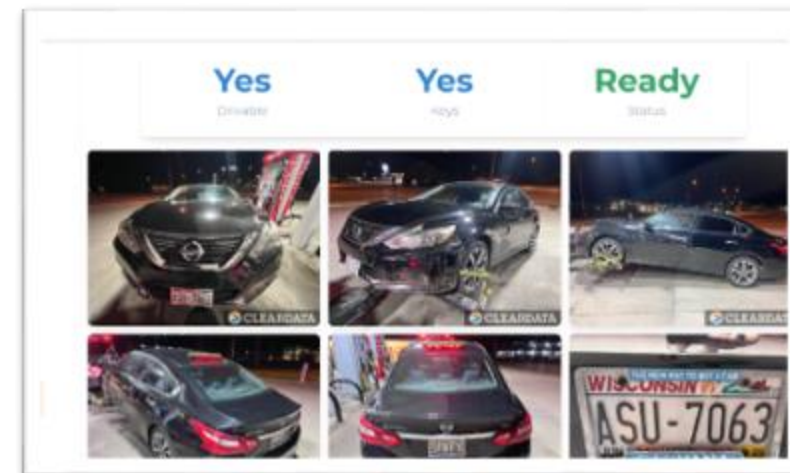


Physical Vulnerabilities

- More Repo volume = more offsite lots = more complexity and barriers to secure
- Utilize layers of security: ensure the perimeter, entrances, building doors, and windows are well lit. Install alarm surveillance systems.
- Organize and secure sensitive information, and protect PII

Vulnerabilities in People, Processes, Policies

- Use the Systems in Place 100% of the time
 - Communicate through secure, trusted platforms
 - e.g. ClearData securely notifies integrated Transport Partners
 - Online scheduling creates digital record, does not allow double booking
 - Modern transport providers have their own branded App.

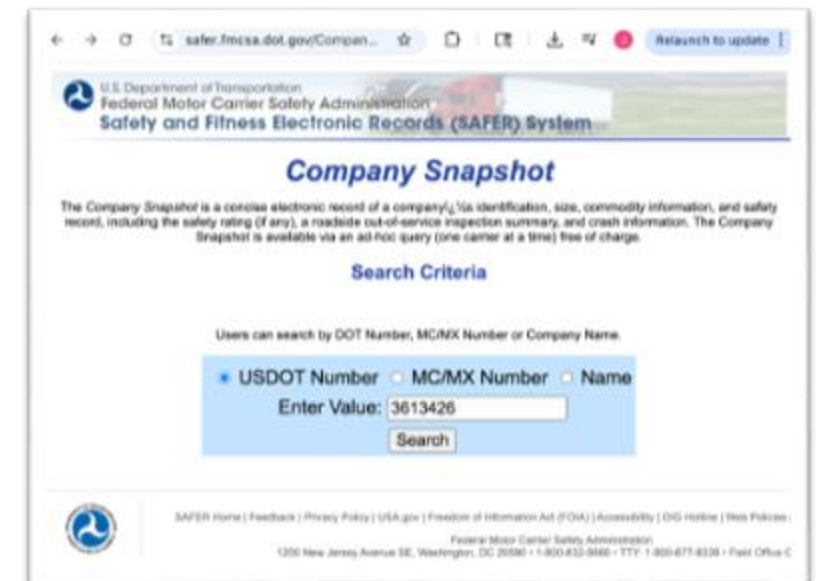
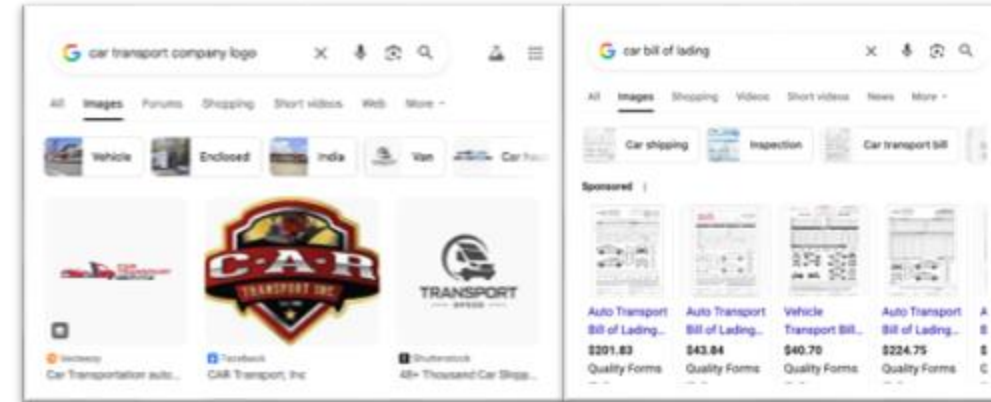


Updated statuses trigger transport in system through secure integrations

Vulnerabilities in People, Processes, Policies

- Harden Processes
 - Do not accept paper BOLs
 - Demand complete, clear, CONSISTENT documentation
 - Verify the Shipper and Destination
 - Sometimes an unsuspecting Transporter
 - Destination should be Auction!
- Verify the Transporter
 - Does Transporter, Driver, DOT, Truck Identifier, Insurance, Driver's License information all match what is in the system?
 - How long have they been in service?
 - Ratings, complaints?
 - <https://safer.fmcsa.dot.gov/CompanySnapshot.aspx>
- Do not accept manual change order requests
- Hold partners accountable
 - Reputable, insured, vetted partners

Paper documents are easier to forge



Vulnerabilities in People, Processes, Policies

- **When in doubt, communicate!**
 - **See something, say something**
 - Lender, Forwarder, Transport Broker, ARA, Law Enforcement

Time is of the essence!

<https://www.fbi.gov/investigate/transnational-organized-crime/cargo-theft>

Call 911 if you are in immediate danger.

File a police report with your local or state law enforcement agencies.

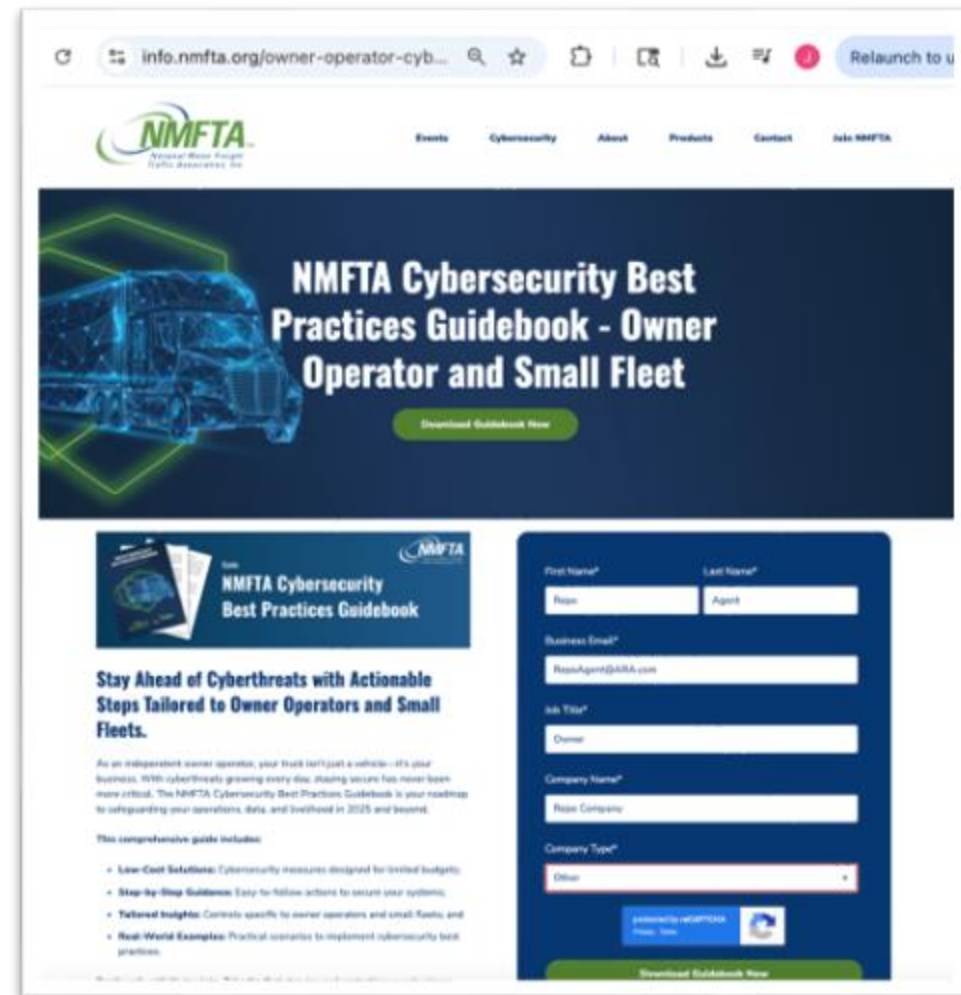
Call 1-800-CALL-FBI (1-800-225-5324).

Submit a tip online at ic3.gov or tips.fbi.gov.



Vulnerabilities in Technology

- Cybersecurity Hygiene
 - Credential and Password Management
 - Who still has an account?
 - No sharing accounts
 - Your login/password information is likely on the dark web (unfortunately, we've seen it)
 - Training
- Resources
 - <https://info.nmfta.org/2025-supply-chain-cybersecurity-trends>
 - Targeted to the resource-constrained Small Business



----- Multiple Tiers

Consumable, bite sized,
recommended actions

Prerequisites: Owner-Operator Controls - Tier One	7
OOSF.01.1 – Keep Software and Operating Systems Updated	7
OOSF.01.2 – Back Up Important Files	8
OOSF.01.3 – Use Strong, Unique Passwords	9
OOSF.01.4 – Require Passwords on All Devices	10
OOSF.01.5 – Require Multi-Factor Authentication	11
Initial: Owner Operator Controls - Tier Two	12
OOSF.02.1 – Basic Cybersecurity User Awareness Training Program	12
OOSF.02.2 – Deploy Endpoint Detection and Response Software	13
OOSF.02.3 – Have an Incident Response Plan	14
OOSF.02.4 – Secure Wireless Networks	15
OOSF.02.5 – Implement a Least Privilege Account Access Policy	16
Intermediate: Owner Operator Controls - Tier Three	17
OOSF.03.1 – Inventory and Classify All Business Data	17
OOSF.03.2 – Designate Cybersecurity Roles and Responsibilities	18
OOSF.03.3 – Layered Network Access Controls	19
OOSF.03.4 – Internal Network Segmentation	20
OOSF.03.5 – Virtual Private Network Required for all Remote Access	21
OOSF.03.6 – Documented Hardware and Software Inventory Management	22
OOSF.03.7 – Configure Email Security	23
OOSF.03.8 – Encrypt all Devices	24
OOSF.03.9 – Enable Detailed Security Logging	25
OOSF.03.10 – Software Version Control and End of Life Management	26
Advanced: Owner Operator Controls - Tier Four	27
OOSF.04.1 – Security Incident and Event Management Solution	27
OOSF.04.2 – Secure Baseline Configurations or Device Images	28
OOSF.04.3 – Network Intrusion Detection System	29
OOSF.04.4 – Formalized, Documented Cybersecurity Policies	30
OOSF.04.5 – Regular Assessments and Exercises	31
OOSF.04.6 – Zero-Trust Architecture	32
OOSF.04.7 – Mobile Device Management Solution	33
OOSF.04.8 – Prioritized Risk Register	34
OOSF.04.9 – Documented Change Control Process	35
OOSF.04.10 – Network Intrusion Prevention System	36

----- What Agents Should Do

Useful Links

1. Sign up directly with the Transport Brokerage who has a relationship with the Lender/Forwarders

And/Or

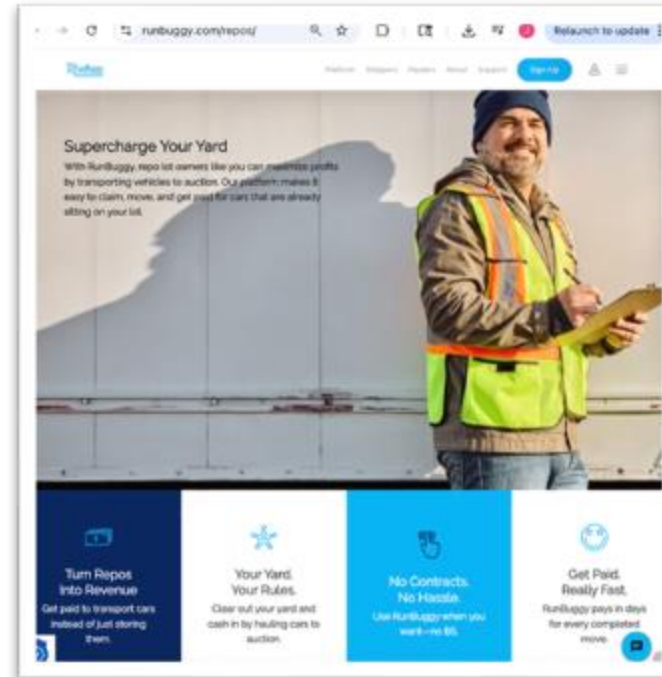
2. Recommend a Trusted Transporter

RunBuggy:

RunBuggy.com/repo

Montway:

Jack.Dimkov@Montway.com



runbuggy.com/repo/

Platform Shippers Haulers About Support Sign-Up

Start turning parked cars into profit today.

Filling out the following information will help us move units from your lot in a timely manner.

1. Business Overview
2. Transportation Preferences
3. Verification Preferences
4. Appointment Preferences
5. Self Transport Details
6. Other Helpful Information

Business Overview

Company Name *

Calls to action

Harden your system of People, Process, Technology

Use the secure systems in place

Step up your own Processes

Sign up with Transport Company directly

1. Move the cars **yourself**
2. Designate your **preferred** Transporter
3. Receive **secure notifications and updates**

Communicate

See something, say something

Thank You

For more information, please contact

Jason Kong | Jason.Kong@RunBuggy.com

How We Help Keep Your Vehicles Secure

- ***In-System Visibility & Digital Documentation***
- ***Zero-Trust Security***
 - **Passwordless Authentication** – No shared passwords, reducing the risk of cyber fraud.
 - **Advanced Encryption & Continuous Monitoring** Our in-house security team actively monitors for suspicious activity, exceeding cybersecurity standards.
- ***Robust Transporter Vetting and Monitoring***
 - **DOT Compliance & Safety Checks** – We ensure transporters meet federal safety and operational regulations.
 - **Insurance Verification** – Every carrier must maintain the required coverage before moving a vehicle.
 - **Business Validation** – verify company credentials, eliminating fraudulent operators before they enter the marketplace.

----- Robust Safety and Security

How Do I Know I'm Releasing the Vehicle to the Right Transporter?

A

Zero-Trust System Architecture

RunBuggy uses passwordless authentication.

All users required to have their own unique login, including Drivers: **no password sharing**

Security by design: advanced encryption and continuous activity monitoring by in-house Security Team

Award winning cybersecurity thought leadership, exceeding SOC2, NIST, and CSF requirements



Interactive IP and threat map showing connections to our services and adversaries we are monitoring or blocking

For a deeper look, visit runbuggy.com/security

B

Robust Transporter Vetting and Monitoring

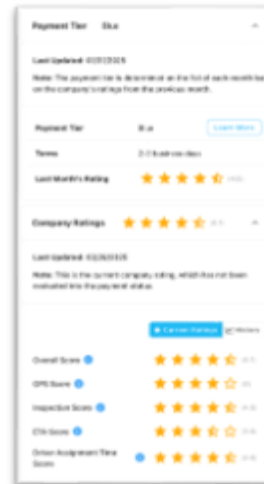
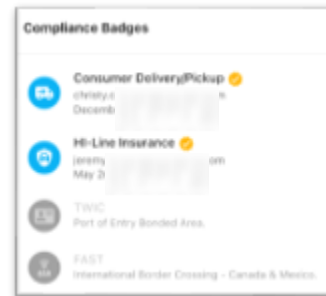
Transporter vetting and verification is a condition of participating in Marketplace

Includes:

- **Time** in Operation
- Required **Operating Authority** and **Insurance**
- Other monitoring criteria including background checks

Compliance Badges and Transporter Ratings

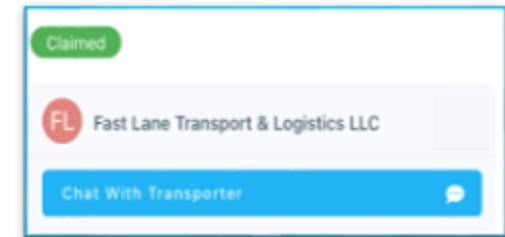
- Heightened requirements for selected moves
- Objective ratings



C

Real Time Transparency and Digital Documentation

Shipper should only release the vehicle to the Transportation company and driver currently displayed in RunBuggy platform



Authentic Bills of Lading are generated by signatures in the **RunBuggy Mobile App**

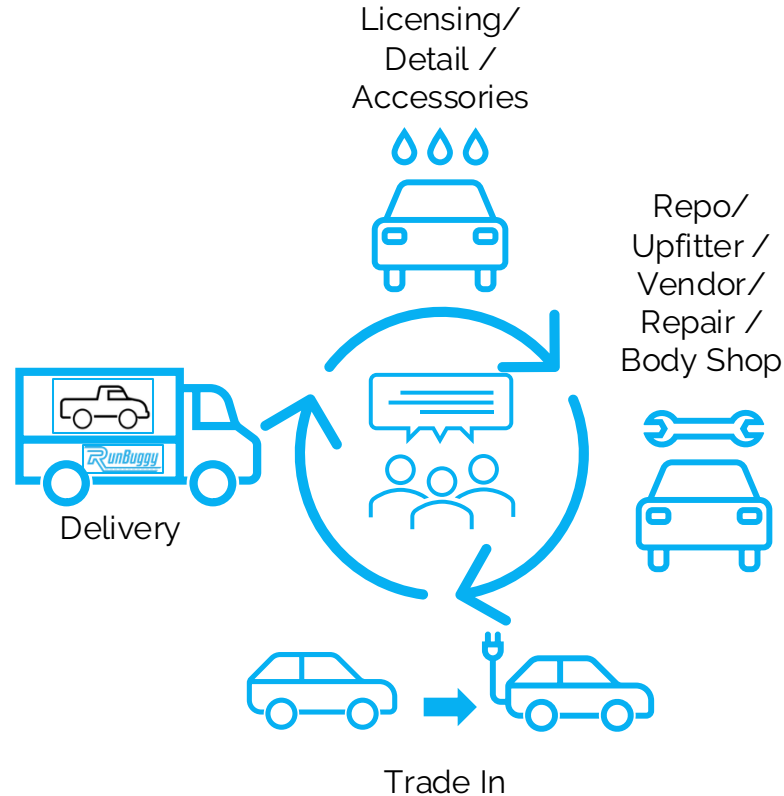


3rd Party Portal: Vehicle Readiness Confirmation and Transporter Verification

Delivered to You Directly

The interface displays the RunBuggy logo at the top. Below it, there are three main sections: Order #5-21136, VIN 1FAGP8529N450, and Vehicle Ford Mustang (2022). Under the VIN section, there is a Pick-up Address: Suni, 15330 Palmdale, CA 91356, and a field for the driver's name. A large text box in the center says "Vehicle is ready for transport". At the bottom, there are two buttons: "Edit" and "Confirm Ready".

Confirm Drivable | Ready | Keys



3rd Party Portal **coordinates multiple external and internal stakeholders and “get ready” functions;** vendors, transporters, customers

The page shows the RunBuggy logo and Order # 1-11229. It includes a "Delivered On" date of Wednesday, October 01, 2025, at 11:01 AM PDT. The "Shipment Overview" section states "Your order has been delivered!" on October 01, 2025, at 11:01 AM PDT. It lists two items: "Signature provided for drop off inspection" and "Driver has arrived at drop off location". The vehicle details are: 2025 Jackson Pike, Grove City, OH 43125, USA. The vehicle is a TOYOTA TACOMA TRD OFFER 4X4 DOUBLE CAB with VIN 3TMCZ5AN090218644. There are buttons for "Download Report" and "Download PDF".

Confirm Official Transport Company and Driver

What Agents Should Do

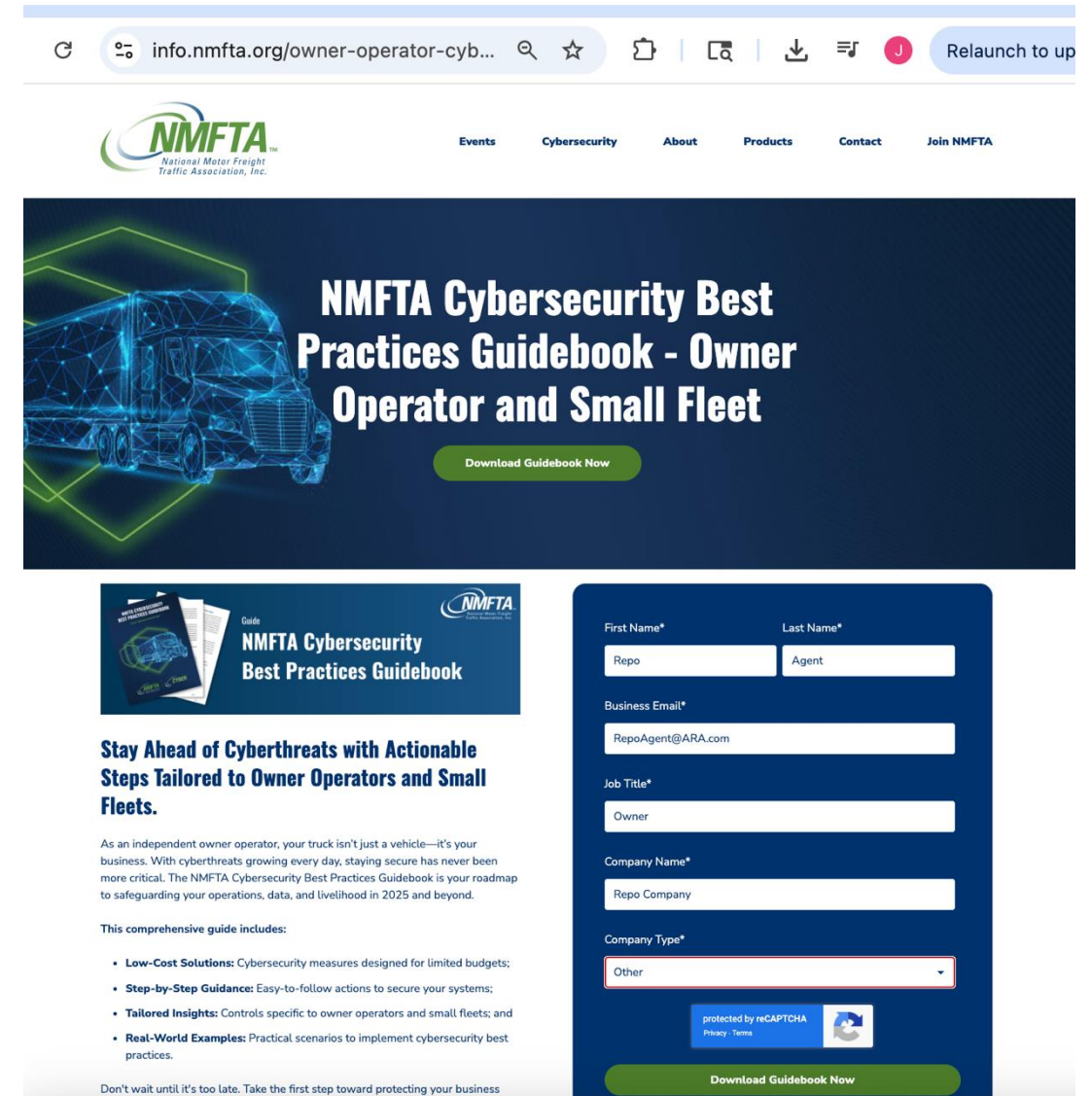
Useful Links

<https://info.nmfta.org/nmfta-cybersecurity-best-practices-guidebooks>

<https://safer.fmcsa.dot.gov/CompanySnapshot.aspx>

<https://RunBuggy.com/repos>

<https://www.nist.gov/cybersecurity-and-privacy>



The image shows a web browser displaying the NMFTA Cybersecurity Best Practices Guidebook landing page. The browser's address bar shows the URL: `info.nmfta.org/owner-operator-cyb...`. The page features the NMFTA logo (National Motor Freight Traffic Association, Inc.) and navigation links for Events, Cybersecurity, About, Products, Contact, and Join NMFTA. The main banner is dark blue with a wireframe truck illustration and the text: "NMFTA Cybersecurity Best Practices Guidebook - Owner Operator and Small Fleet". A green button labeled "Download Guidebook Now" is visible. Below the banner, there is a section titled "Stay Ahead of Cyberthreats with Actionable Steps Tailored to Owner Operators and Small Fleets." which includes a brief introduction and a list of guidebook features: Low-Cost Solutions, Step-by-Step Guidance, Tailored Insights, and Real-World Examples. To the right, a registration form is displayed with fields for First Name (Repo), Last Name (Agent), Business Email (RepoAgent@ARA.com), Job Title (Owner), Company Name (Repo Company), and Company Type (Other). The form is protected by reCAPTCHA and includes a "Download Guidebook Now" button at the bottom.

info.nmfta.org/owner-operator-cyb... Relaunch to up

NMFTA
National Motor Freight
Traffic Association, Inc.

Events Cybersecurity About Products Contact Join NMFTA

NMFTA Cybersecurity Best Practices Guidebook - Owner Operator and Small Fleet

Download Guidebook Now

Guide
NMFTA Cybersecurity Best Practices Guidebook

Stay Ahead of Cyberthreats with Actionable Steps Tailored to Owner Operators and Small Fleets.

As an independent owner operator, your truck isn't just a vehicle—it's your business. With cyberthreats growing every day, staying secure has never been more critical. The NMFTA Cybersecurity Best Practices Guidebook is your roadmap to safeguarding your operations, data, and livelihood in 2025 and beyond.

This comprehensive guide includes:

- **Low-Cost Solutions:** Cybersecurity measures designed for limited budgets;
- **Step-by-Step Guidance:** Easy-to-follow actions to secure your systems;
- **Tailored Insights:** Controls specific to owner operators and small fleets; and
- **Real-World Examples:** Practical scenarios to implement cybersecurity best practices.

Don't wait until it's too late. Take the first step toward protecting your business

First Name* Last Name*
Repo Agent

Business Email*
RepoAgent@ARA.com

Job Title*
Owner

Company Name*
Repo Company

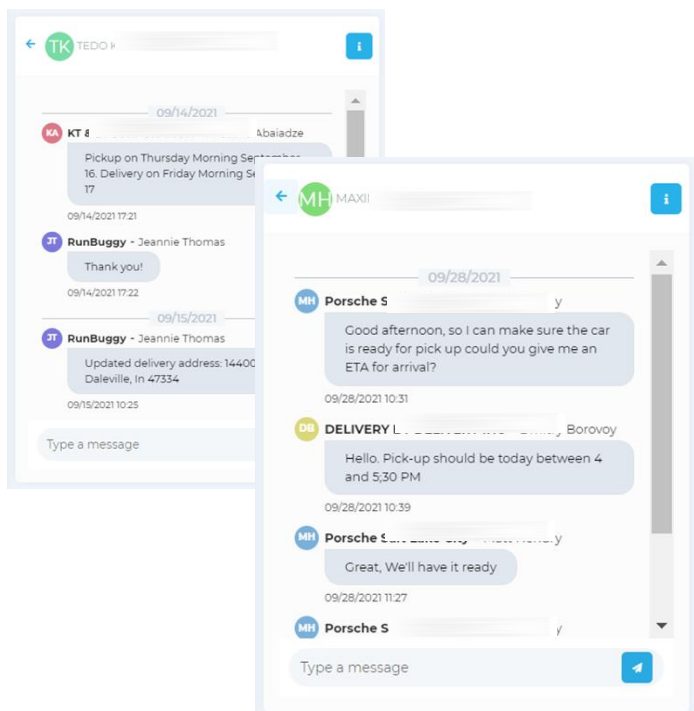
Company Type*
Other

protected by reCAPTCHA
Privacy Terms

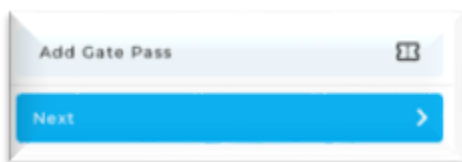
Download Guidebook Now

Integrated Communication Tools

Driving Better Experiences



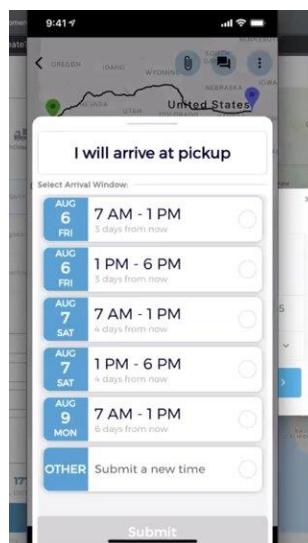
Active order chat – shipper/carrier



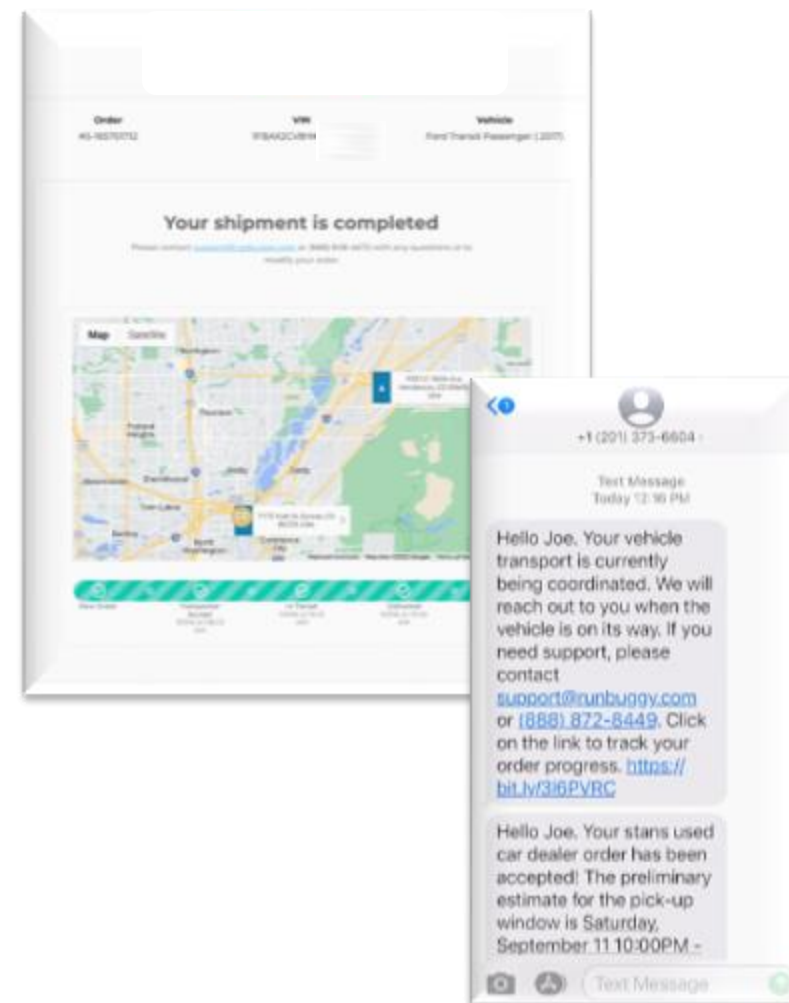
Gate Passes or releases attached to each order



Carrier location tracking



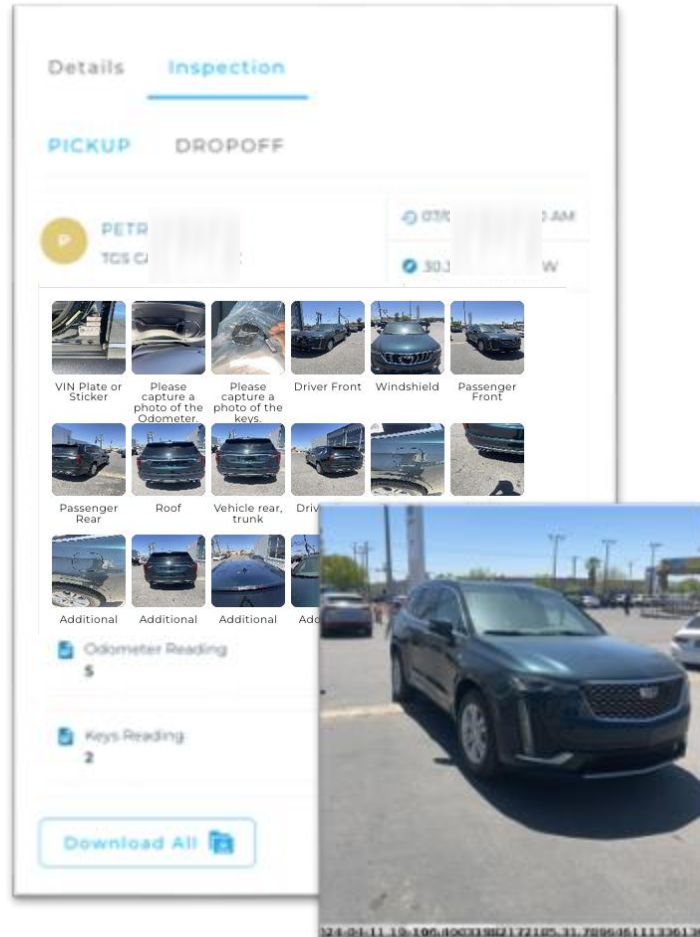
Dynamic, VIN-level Transporter ETA



White-labeled customer scheduling & updates

Order Transparency

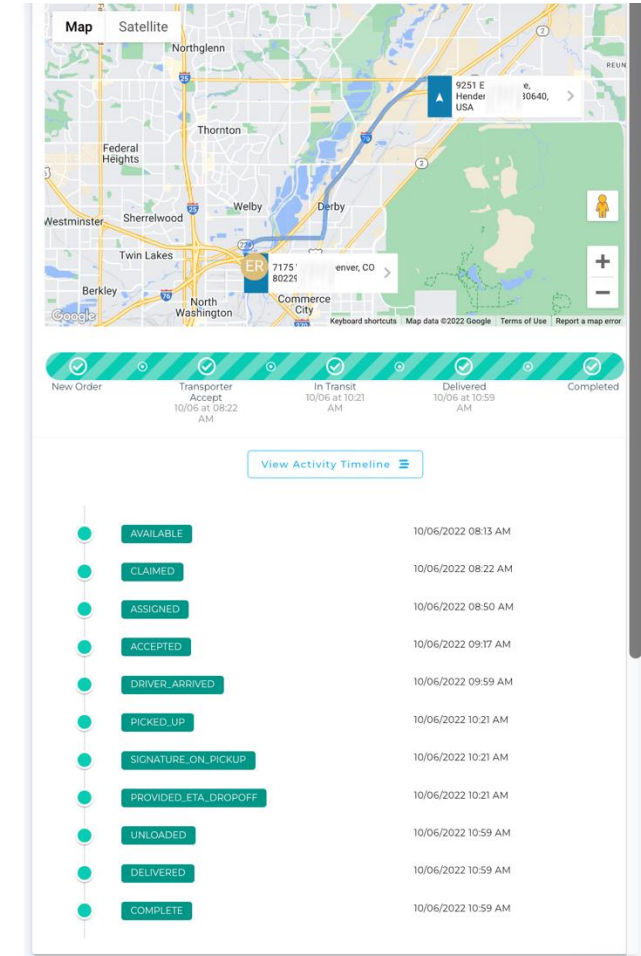
All Events and Data Can Be Pushed to Internal and External Stakeholders



Pickup and dropoff pictures:
geotagged and time stamped



Digital Bill of Lading



Event statuses captured and
communicated in real time