AMERICAN
TRUCKING
ASSOCIATIONS

80 M St. SE, Ste. 800, Washington, DC 20003 ★ www.trucking.org

June 18, 2024

Mr. Jeff Secrest
Chief, Registration Division, Office of Registration
Federal Motor Carrier Safety Administration (FMCSA)
United States Department of Transportation
1200 New Jersey Avenue SE
Washington, DC 20590

**Re: Information Collection Request on Upgraded FMCSA Registration System**

Dear Mr. Secrist:

The American Trucking Associations (ATA)[1] and ATA's Moving and Storage Conference (MSC)[2] thanks the Federal Motor Carrier Safety Administration (FMCSA) for the opportunity to provide public comment on the Agency's plan to upgrade its existing Unified Registration System (URS) to a new online FMCSA carrier registration system. ATA supports FMCSA's efforts to bolster the safety, security, and efficiency of its existing carrier registration system, and emphasizes the urgent need to implement measures, including but not limited to those lent by a modernized registration system, to prevent escalating fraud and cargo theft trends in the industry.

As the largest national trade association representing the interests of the trucking industry with more than 37,000 members, ATA remains focused on the issue of fraud and theft in the trucking industry. ATA continues to engage in efforts to mitigate and prevent the damage incurred by carriers who fall victim to such fraud and, subsequently, consumers across the country. According to commercial cargo theft and recovery network CargoNet, cargo theft rose a substantial 46 percent in the first quarter of 2024 as compared to the first quarter of last year and represented an estimated $154.6 million in stolen goods.[3] While these figures are likely an underrepresentation of the true magnitude of the issue given the decentralized, inconsistent nature of cargo theft reporting, ATA has become keenly aware of increasing cargo theft cases – often linked to strategic motor carrier and broker fraud undertaken by criminal organizations – experienced by our membership. In many cases, these illegitimate actors falsify or use counterfeit information within FMCSA's registration system to illicitly obtain USDOT numbers or verify other information (i.e., operating authority, cargo, and liability insurance information) to hold hostage or steal legitimate carriers' freight. In this same vein, ATA has heard about the simplicity of obtaining a USDOT number, accessing carrier information, and registering as a fake driver or carrier through the existing URS given its limited verification steps. Legitimate carriers, including those represented by ATA, are faced with the burden of expending extensive time and financial resources to prevent such fraud and theft, or other leaving themselves vulnerable to such risk.

Unfortunately, limited means to identify, prevent, and/or hold these bad actors legally or financially accountable exist. These fraudulent entities also compromise FMCSA's ability to monitor the safety of

[1] ATA is a united federation of motor carriers, state trucking associations, and national trucking conferences created to promote and protect the interests of the trucking industry. Directly and through its affiliated organizations, ATA represents motor carriers in the United States encompassing every type and class of motor carrier operation.
[2] ATA's Moving and Storage Conference is the leading national organization representing household goods moving companies and industry suppliers, as well as various state moving and storage associations. The Conference sets household goods government affairs policy positions on Capitol Hill, promotes industry unity, and provides a forum for intra-industry debate and collaboration.
[3] "2024 First Quarter Supply Chain Risk Trends Analysis," CargoNet, https://www.cargonet.com/news-and-events/cargonet-in-the-media/2024-q1-theft-trends/.

active carriers on our nation's roadways and threaten the business viability of legitimate carriers, brokers, and their customers. ATA emphasizes the need to safeguard and promote legitimacy and security throughout the registration lifecycle of carriers, at all touchpoints between FMCSA and regulated entities.

Additionally, "chameleon carriers" – an FMCSA-registered business entity that has shut down for reasons including but not limited to a poor safety record or numerous violations, difficulties obtaining insurance coverage, or a history of financial issues applies for a new USDOT number under a new business identity – continues to surge and is especially prevalent in the moving and storage industry. Chameleon carriers can then continue operating under a new business identity and USDOT authority, free from previous business concerns. By evading reputational and safety standards, chameleon carriers can compromise roadway safety and efforts to elevate Commercial Motor Vehicle (CMV) industry safety standards.

ATA commends FMCSA's recognition of these issues and efforts to address mounting fraud in the industry through its proposed transition to a new FMCSA Registration System. FMCSA's proposed enhancements reflect a significant step towards modernizing and securing the registration process for the CMV industry. ATA also recognizes FMCSA's swift interim efforts to bolster the current URS security and identity verification and thwart fraudulent actors until the new system is live. In response to FMCSA's Information Collection Request (ICR), ATA provides the following recommendations and considerations to further strengthen the system against fraudulent activities.

*Streamlined Access & Use for Legitimate Carriers without Undue Regulatory Hurdles*

ATA believes FMCSA's proposed adoption of the new FMCSA Registration System (FRS) offers a critical path towards effectively mitigating and reducing fraud in the CMV industry. While ATA recognizes these changes will inevitably increase barriers to entry for businesses seeking to register with FMCSA, we urge FMCSA to ensure regulatory and technical requirements initiated under this ICR and any future rulemaking processes do not overburden legitimate carriers and brokers in their attempt to meet registration and safety requirements, or unintentionally disincentivize businesses from registering altogether. Regulations to strengthen the FMCSA registration process and systems must balance a heightened level of data security with streamlined, easy-to-understand procedures. FMCSA must also undertake outreach and engagement to ensure new requirements and processes – as well as their purpose – are widely understood by FRS users and not seen as government overreach or privacy infringement. For example, FMCSA should emphasize that increased identity and business verification steps – such as requiring applicants to submit government-issued identification (i.e., driver's license) – are intended to protect individuals and companies and prevent identity theft, rather than a means for FMCSA to steal or abuse personal information.

Further, ATA supports FMCSA's proposal to sunset existing IT systems and consolidate the existing registration process, including all forms and certifications, into a single user-friendly online system. Before this begins, FMCSA must develop and communicate a clear set of expectations around the sunsetting process – including timelines, user responsibilities, and transition requirements – to the vast ecosystem of system users. FMCSA must also ensure users can continue accessing necessary data from the previous system throughout the transition, or otherwise clearly communicate timeframes when data and/or systems will be inaccessible.

While higher barriers to entry and enhanced security are central to preventing fraudulent actors from accessing and exploiting sensitive carrier information, ATA cautions FMCSA from making the system onerous or overly complex, defeating the purpose of its use. Some members and users of the existing URS report that the online application process is archaic, complex, and lengthy, and reviewing online application materials ahead of time is nearly impossible without logging in as a prospective applicant. FMCSA must take heed not to build a new system with the same issues and simultaneously ensure that the regulatory barriers incorporated into the new FRS do not place an extreme burden on legitimate businesses. Authentication processes should also be built to accomplish their goals of system security and identity verification without creating barriers to use for legitimate users through excessively difficult or time-consuming steps.

To the extent the new online platform may be integrated with legitimate carriers' existing human resources or IT systems (i.e., Oracle PeopleSoft, ADP Workforce, Workday), FMCSA can promote ease of access for users and ensure user legitimacy. In doing so, employees who have left a registered company can be automatically removed from accessing the system under that carrier's business identity, preventing potential impersonation or unauthorized access. To further streamline the user experience, the FRS may benefit from featuring an internal dashboard upon login where applicants can see required and completed tasks and past account activity.

Finally, FMCSA should address common access issues that occur when an employee with primary URS access leaves a company. To ensure carriers and all user types can continue accessing critical business information, FMCSA should develop streamlined processes and procedures for recovering login access in these instances and, more urgently, establishing practices to prevent this from occurring in the first place (i.e., developing umbrella accounts for the business entity, rather than on an individual basis).

*Enhanced Identity Verification & Security Measures*
ATA commends FMCSA's immediate steps to begin strengthening the security and identification processes built into the existing URS and recognizes that robust identity and business verification processes are crucial to the long-term integrity of the registration system and its data. As noted, the ease of obtaining a USDOT number or other identifying information under the current URS has enabled illegitimate actors to broker loads on behalf of an impersonated entity and ultimately carry out cargo theft. FMCSA's plans to bolster security and heighten barriers to entry in the registration process through a consolidated online-only registration process, smart logic to detect and prevent inaccurate or duplicative data entries, identity verification via checks for matched entities, and enhanced vetting of all applicants offer a key pathway towards reducing these incidents. By rolling all registration processes and forms into a single FMCSA interface, registrants will have an incentive to regularly access the FRS portal, in turn creating additional opportunities for legitimate users to ensure account security and accuracy of company information, as well as detect and report any suspicious activity.

FMCSA should consider additional ways to build enhanced identity and business verification and security features into the new FRS, including:

- Multi-factor authentication requirements for all users;
- Advanced government identification and document (i.e., passport, driver's licenses) verification technologies that are checked in real-time against official databases for all new registrants.
- Integrated interfaces between FRS and company credentialing systems (i.e., human capital management/payroll systems) to streamline the login process and allow for real-time checks and limits on user access – i.e., blocking access to employees who have since left a registrant's organization.
- Enhanced registration information cross-referencing with other federal and state databases (i.e., IRS/tax records, state business registration).
- Cross-referencing applicants and business information with databases of business complaints and proven misconduct (i.e., via Better Business Bureau, Small Business Administration Inspector General, and law enforcement authorities).
- Improved vetting processes for all applicant types, including brokers and freight forwarders, that involve both human and artificial intelligence-driven screening and vetting of applications.

Additionally, a robust cybersecurity framework is essential to protect the new FRS from cyber threats and security breaches. ATA recommends that FMCSA deploy end-to-end encryption and strict access controls as well as proactively conduct regular penetration testing and vulnerability assessments to identify and address potential security weaknesses.

*Improve Data Quality & Accessibility*

Underlying enhanced identity and security measures, ATA emphasizes the importance of ensuring the accuracy and reliability of data within the new registration system for effective fraud prevention and operational efficiency. Based on anecdotal evidence from members as well as ATA's internal use of FMCSA URS data, duplicate or illegitimate registrant information is common – for instance, numerous carriers register at a single address located in an apartment complex or strip mall, all using a single email address. To address these issues, FMCSA should implement rigorous data validation processes at the point of entry to minimize errors and inconsistencies; conduct regular data audits to identify and correct any inaccuracies, ensuring that all records are up-to-date and accurate; and utilize advanced data analytics to continuously monitor data quality, identifying potential discrepancies and addressing them promptly. Eliminating the use of paper forms and application materials and transitioning towards a fully online registration platform will support efforts to catch erroneous data entries in real-time, potentially weeding out bad actors at the source. Additionally, because a significant amount of data in the URS may be inaccurate or otherwise unreliable, FMCSA would benefit from a full audit and clean-up of the existing database. This may also serve to deactivate and remove inactive accounts and associated USDOT numbers that are susceptible to being exploited by fraudulent actors.

ATA also recommends building into the system a feature that checks applicant entries against existing FMCSA databases to identify and flag data discrepancies or if that entity has had previous revocations. To further combat fraud and chameleon carriers from counterfeiting information, FMCSA should commit the necessary resources to create an authoritative data system by ensuring these databases are updated in real-time. This includes but is not limited to ensuring email and physical mailing addresses used during the registration process are valid and matching a carrier's reported fleet size to its number of drivers before granting access. FMCSA should also cross-reference and audit carrier data across its various platforms and databases (i.e., FMCSA Licensing & Insurance, SAFER, URS, and Registered Mover databases) as it is common for each of these platforms to display different information for a single entity across platforms.

Finally, though currently external to FMCSA's URS, ATA recommends tying the FMCSA inspections portal and DataQs system more closely with the proposed FRS. Currently, when a carrier is attempting to remediate their CSA/SMS scores following a poor inspection caused by an entity falsely acting under the legitimate carrier's USDOT number, they must do so through the DataQs process to have FMCSA remove the inspection record. This not only requires carriers to expend time and resources to expunge illegitimate inspection data but also places a burden of proof on the carrier that a driver was impersonating the company. Under the current FMSCA portal, inspection data may take days or weeks to populate, further exacerbating the issue. FMCSA should explore ways to align and streamline all data a carrier may need to access – from registration to inspection – under one real-time, easy-to-use platform and portal to enhance monitoring and alleviate some of the burden currently placed on carriers. Investigating alternative solutions to the DataQs process for carriers who have fallen victim to fraud and whose safety rating may have suffered as a result should accompany such efforts.

*Operating Authority & USDOT Number Issuance*

ATA supports, in theory, FMCSA's proposed steps to eliminate MC numbers and transition towards using USDOT numbers as the sole identifier of operating authority for carriers. If MC numbers are eliminated, FMCSA needs to first investigate and understand any unintended consequences associated with doing so and avoid creating a situation that inadvertently bars some carriers' ability to operate. Allowing only one USDOT number per registrant may reduce opportunities for fraudulent activities and clarify accountability by preventing entities from creating multiple identities to circumvent regulations or mask poor safety records. If adopted, we recommend that FMCSA consider implementing robust policies and verification processes to enforce the one USDOT number per registrant rule. Nevertheless, FMCSA must account for legitimate motor carriers who seek to obtain multiple USDOT numbers based on their businesses' needs. For instance, some motor carriers operate under the same parent company but have multiple USDOT numbers for each pillar of operation (i.e., Bob's Local Delivery vs. Bob's Over the Road Delivery). Additionally, FMCSA must establish a clear process for entities that legitimately require updating or changing their USDOT number due to significant business changes – ensuring that these cases are thoroughly reviewed and verified. These efforts must be reinforced by ongoing system monitoring and auditing to ensure compliance with this rule, taking prompt action against any entity attempting to obtain multiple USDOT numbers fraudulently.

*Establish Thresholds for Entry*
In place of the current operating authority certification ("MC," "FF," or "MX" numbers), it is critical to establish clear and stringent thresholds for registering with the FMCSA system to ensure that only legitimate and qualified entities are allowed to operate, ultimately holding all new and existing registrants accountable to equal safety and operational standards. In defining specific criteria for registration eligibility, FMCSA should consider carriers, brokers, and other regrants' operational and financial history and compliance with FMCSA safety standards. For new carriers obtaining a USDOT number for the first time, they must remain subject to the New Entrant Safety Assurance program to ensure compliance monitoring during their first few months of operation. Additionally, to the extent resources allow, FMCSA may consider developing a tiered registration system that categorizes entities based on safety and fraud risk levels, with higher-risk entities subject to more rigorous verification and monitoring processes. Again, FMCSA should strike a balance between enhanced barriers to entry for fraudulent entities and ensuring these barriers do not disincentivize legitimate entities from going through the registration process altogether.

*FMCSA Registration System (FRS) Implementation*
The implementation of the FRS is a vital move towards reducing administrative burdens and eliminating redundancy by consolidating various forms into a single, streamlined online process. To ensure its initial and ongoing success, FMCSA must take steps to ensure a smooth transition away from the URS, with comprehensive support and clear communication provided to all stakeholders to facilitate their adaptation to the new system.

Educating existing URS users and prospective registrants on the new system's functionality and goals of modernization and fraud prevention is vital for ensuring widespread adoption and effective use. Upon rollout of the new FRS, FMCSA should consider developing comprehensive training programs and resources, including webinars, tutorials, and dedicated technical assistance and customer service, to assist users during the transition period. ATA also suggests launching an ongoing awareness campaign that highlights the benefits of the new system and provides updates on best practices for maintaining security and compliance. FMCSA should call upon relationships with industry partners – including ATA and its affiliated conferences and councils, to promote widespread awareness.

Importantly, FMCSA should remain flexible and nimble to allow for long-term improvement in the process. FMCSA should allow room to examine how proposed registration modernization unfolds, improve areas that are not working well, address any unintended consequences, and incorporate additional measures to continue its efforts to combat fraud and chameleon carriers. This will require FMCSA to commit to ongoing engagement with system users and CMV industry stakeholders to gather feedback throughout and following the transition process.

*Create an Ecosystem of Fraud Prevention Beyond Registration System*
ATA reiterates its support of FMCSA's transition to a new online registration system that is designed around an improved user experience and identity security and emphasizes the need for these steps to be undertaken within the context of a broader ecosystem of heightened fraud prevention and remediation. ATA commends

FMCSA's recognition of the urgency of this issue and the immediate steps the Agency has taken to tackle fraud until a new registration system can be implemented. To complement and support the success of the planned registration system upgrade, FMCSA should also consider bolstering "wraparound" fraud prevention activities including education and outreach to the CMV community; reporting mechanisms, communication, and customer support; and ongoing auditing and monitoring to identify and thwart bad actors. While improved online systems offer built-in validation and smart logic to flag potential fraud, FMCSA must support system improvements with human-driven monitoring and auditing to detect high-risk profiles and catch redundancies or discrepancies in registrant information (i.e., false or duplicate names, mailing or email addresses, or other personally identifying information) or activity (i.e., multiple failed login attempts or PIN requests from a centralized IP address) indicating a fraudulent attempt. FMCSA should also dedicate resources to better understanding and identifying *sources* of fraud, their prevalence, and the extent to which fraudulent practices are committed by individuals acting within legitimate organizations (i.e., brokers, freight forwarders, third parties, and intermediaries involved in the application process). FMCSA should build out a dedicated inspection and vetting program to ensure brokers and freight forwarders who gain access to sensitive company information are legitimate. FMCSA should also enhance its authority and ability to investigate entities that evade the registration process or otherwise operate outside of their legal authority. ATA believes these responsibilities may be appropriately housed within FMCSA's proposed registration fraud team, as announced during the May 29th FMCSA Registration Modernization Stakeholder Day.

Additionally, FMCSA should engage in ongoing interagency collaboration and industry partnerships to further establish a holistic approach to fraud prevention. For instance, establishing a formal advisory board comprising representatives from federal and state agencies, industry organizations, and cybersecurity experts may offer ongoing guidance and oversight throughout the lifetime of the new FRS.

While these countermeasures and industry supports will inevitably require additional staffing and resources, ATA believes they will ultimately result in cost savings when considering the time and resources required to investigate fraud and cargo theft that has already occurred, in addition to the material loss experienced by carriers – and, in turn, their customers – who fall victim. Complimenting the implementation of a new online registration system will further heighten barriers to entry and access for individuals acting in bad faith while offering effective, accessible customer support to report suspected fraud and seek corrective action for those carriers, brokers, and other entities who fall victim. FMCSA must commit to a culture of continuous improvement and comprehensive prevention efforts beyond the scope of an updated registration system to ensure long-term success and registrant satisfaction.

ATA appreciates the opportunity to weigh in and support this important initiative to mitigate the growing issue of fraud in the CMV industry and transition towards a modernized online registration system. Please do not hesitate to reach out if we can be of further assistance in FMCSA's design and implementation of this new system.

Sincerely,

Brenna M. Lyles

Brenna Lyles,
Director, Safety Policy
American Trucking Associations

Sincerely,

Jon Samson
Vice President, Conferences
American Trucking Associations