NAPA RIVER INSURANCE SERVICES®

RISK IN SIGHT

TRANSPORTATION ISSUE

FALL/WINTER 2017

Napa River: How We Help Solve the Transportation Claims Puzzle

Driver fatigue. Road conditions. Inadequate training. All of these are significant factors which play a role in driving your company's losses.

Napa River Insurance Services, Inc. is dedicated to providing the data and training resources essential to solving the puzzle of your organization's transportation claims. We work with you to identify and collect the data points important to your business as soon as a claim occurs, which not only helps ensure greater accuracy in the claim details but also helps preserve important facts for risk management and claims defenses. This information is captured and aggregated within our innovative claims management software, FileHandler™. Our experienced claims staff then uses this data to generate customized loss-run reports for you, our valued clients.

"Our whole life is solving puzzles."
— Erno Rubik

We also offer customized driver training and safety programs through our online Risk Management Center, powered by Succeed®. This comprehensive online resource includes a risk management library with instant access to over 2,000 risk management and safety resources, in addition to a robust HR & Benefits Library, and powerful risk management analytical tools.

The link (https://www.jwsoftware.com/~jwsoftware/staging/fhe_vid_re_scss_pg/) provides a brief overview of the types of custom reports that can be designed within FileHandler and easily emailed to you without the need to continuously log in to the system.

Napa River is committed to working with you and your company to identify each and every aspect of your needs, and together, solving the often daunting puzzle of transportation claims.

Peggy Killeen
Director
Napa River Insurance Services
212.978.2847
pkilleen@napariverinsurance.com

What's Inside:

Advances in Safety: Is Technology the Answer?

Jeffrey K. Davis
Vice President of Safety
Napa River Insurance Services
317.810.2034
jdavis@napariverinsurance.com

In our last issue of *Risk in Sight,* we looked at the importance of people and culture as the first step towards controlling risk in commercial transportation. Professional drivers and those who support them must work together with the common goal of returning home safely from every single trip. Drivers and companies are also charged with the safety of the general motoring public, with whom we share the roads. As professionals, we hold the greater responsibility to avoid trouble on our nation's highways.

As technology has advanced over the last several years, it has increasingly played an active role in accident avoidance or mitigation. At the same time, an ongoing debate has emerged as to whether this technology may actually harm the driver by becoming a distraction.

In a study released in September 2017, the AAA Foundation for Traffic Safety looked at four types of advanced safety technologies available for large commercial vehicles and found each had measurable benefits to highway safety:

LANE DEPARTURE WARNING SYSTEMS

These systems could hold the greatest promise in preventing a number of truck crashes, from simple lane-change accidents to serious roadway departures. Erratic lane tracking or repeated lane departure and correction can also indicate a fatigued driver. Our experience has found lane-change accidents to be the most frequent types of claims for our trucking clients.

By immediately alerting the driver and providing timely telemetric data to the company, corrective action can be taken before this behavior leads to an accident. These systems can also help identify vehicles in truck blind spots and warn the driver before a potential collision. The AAA Foundation study found as many as 6,372 crashes, 1,342 injuries and 115 deaths could be prevented annually if these systems were deployed on all large trucks.[1]

VIDEO-BASED ONBOARD SAFETY MONITORING SYSTEMS (DASH CAMS)

These systems are becoming more widely used to monitor driving behavior through the recording of triggering events. These videos are then used to counsel drivers. We have found that just by having the camera in the unit, drivers become more aware of their driving habits and change behavior so as not to activate the camera. Newer systems are also starting to provide telemetric data that shows performance information on such habits as following too closely, even without a triggering event. The AAA study estimates as many as 63,000 crashes, 17,733 injuries and 293 deaths could be prevented annually by the use of dash cams.[2]

(continued)

AUTOMATIC EMERGENCY BRAKING SYSTEMS

Rear-end accidents are by far the priciest claims we see in both property damage and human cost. The current generation of these systems has proven effective in avoiding or at least mitigating losses by intervening before a driver might have a chance to react. These systems monitor closing rates as the unit approaches a vehicle from the rear. Simple mechanical physics still play a major role in system effectiveness. In the case of a sudden slowing of traffic or another vehicle cutting in front of a truck, the unit still needs adequate room to stop. We do, however, have the opportunity to lessen the impact by having the truck react more quickly to the impending hazard. The AAA study estimates 5,294 crashes, 2,753 injuries and 55 deaths could potentially be prevented annually if these systems were deployed on all large trucks.[3]

AIR DISC BRAKES

This technology is valuable not only to power units, but also trailers. In addition to bringing greater stopping power to the unit, the use of this equipment also contributes to lower long-term maintenance costs. The AAA study found that installing these braking systems on all large truck units could prevent as many as 2,411 crashes, 1,447 injuries and 37 deaths annually.[4]

While both the professional driver and the environmental safety culture we cultivate remain the most import components of avoiding costly accidents, technology has clearly become a tool that benefits our professional drivers. While it will be years before we see the aforementioned technology on all trucks, be sure to at least explore the technological options available when making future purchases.

For more information, you can view a full copy of the AAA study *Leveraging Large-Truck Technology and Engineering to Realize Safety Gains* at AAAFoundation.org.

[1] *Leveraging Large-Truck Technology and Engineering to Realize Safety Gains, AAA Foundation For Traffic Safety, September 2017.*

[2] *Ibid.*

[3] *Ibid.*

[4] *Ibid.*

Communicating With Your Driver: Post-Accident Claim Management

Stephen M. Philleo, J.D.
Director of TPA Claim Operations
Napa River Insurance Services
317.810.2046
sphilleo@napariverinsurance.com

When a driver has an accident, proper safety protocol mandates that the driver immediately report the incident to his/her company. After that, it is important that the company clearly communicates to the driver the next steps and proper procedures that should be followed. Unfortunately, this is not usually the case.

In order to help ensure you are communicating to your driver the proper claim management procedures following an accident, we put together a short list of driver Dos and Don'ts.

DRIVER DOS & DON'TS

DOS

- **DO** always be truthful and extend professional courtesy to law enforcement and investigative personnel at the scene. You should not be combative.
- **DO** remember that your TPA, Napa River Insurance Services, Inc., or excess carrier, Hudson Insurance Company, will be handling the claim and/or suit on the company's behalf. Note that upon initial investigation at the claim stages, our claim investigators and/or defense counsel will not take any formalized statement from you, the driver, since we do not want your information preserved and possibly used as impeachment material in a legal proceeding, deposition and/or trial testimony.
- **DO** advise the company immediately if you are served with any legal papers (suits, citations), since these legal papers require a proper response within a prescribed timeframe.
- **DO** keep the company advised of your current contact information, especially if you are no longer employed at the company and there is a pending accident claim or suit. Your cooperation may be needed for defense at a later date.

DON'TS

- **DON'T** say "I am sorry" at the accident scene. Although this may be a natural reaction, these words can be detrimental in claim and legal handling and can be considered an admission of guilt or liability.
- **DON'T** take photographs of any visible injuries. Those injuries SHOULD NOT be detailed in photos, since graphic injury photos can be used against the company in efforts to bolster the injured parties claim or suit, and may also be portrayed as an insensitive action. The opposite is true in terms of photographing the scene environment—it is fine to photograph placement of vehicle(s), license plate, etc.
- **DON'T** volunteer to speak and give out details of the accident if contacted by any claimant carrier or plaintiff attorney. Any caller should be directed to contact the company.

Although one should take any and all measures to prevent such an incident, accidents will undoubtedly happen. When it does, you will now be prepared to clearly and easily communicate to your driver best practices for claim management.

Do not hesitate to contact your Napa River claim representative if you have any questions or desire further guidance.

Cyber Liability: Today's Rapidly Growing Risk

John Whall
Senior Vice President
Hudson Insurance Group
816.778.0710
jwhall@hudsoninsgroup.com

This is the second article in a series. The first article, which focused on the nature and scope of cyber liability, appeared in the previous edition of *Risk in Sight* located here: https://www.napariverinsurance.com/transportation/overview/

PART TWO:

Ways Your Organization Can Be Harmed

There are many ways that thieves looking for access to personal health information can gain access to a system. They can hack their way in by exploiting security vulnerabilities of a healthcare provider or one of its vendors. They can use socially engineered attacks such as phishing, where spoofed e-mails appear legitimate at first glance but actually trick employees or patients into turning over passwords, granting access to information or unknowingly installing malware on the network. There is also the threat of a rogue employee abusing access privileges. According to a recent Ponemon healthcare study, outside criminal attacks are the primary source of breaches (accounting for an estimated 50% of breaches), while rogue employees accounted for an estimated 13% of breaches.[1]

Last year, an Ohio clinic was hacked and the criminal released approximately 150 GB of medical records, personal information, and financial and other business data. The group claiming responsibility, Pravvy Sector, made no demand for money; it appeared to only be interested in getting attention. Nonetheless, the clinic appears to have incurred significant costs in connection with the breach. News media reported that the clinic sent notification to persons affected and offered to them free credit monitoring and identity protection. An industry database reported that the clinic engaged a forensic technology firm, conducted a new risk assessment, installed an upgraded firewall system and implemented additional safeguards. Given the fact that the data was made public, it was deemed possible that there would be regulatory fines and penalties, and there could be PCI fines/penalties if financial information was involved. The clinic was a respected facility and reputational damage was a concern, thus public relations expenses also may have been incurred.

Ransomware / Malware

Ransomware is the fastest-growing cybercrime across all industries but its growth in the healthcare sector has been explosive. In a ransomware attack, the criminal finds a way to get malware onto the healthcare provider's network in order to either:

(1) take control of the entire network or critical portions of it or

(2) encrypt critical data or records that the facility needs to operate. The criminal then makes a monetary demand, typically in bitcoins for anonymity purposes, in order to restore control of the digital assets to the victim.

Last year, criminal hackers using malware seized control of Hollywood Presbyterian Medical Center's

(continued)

[1] *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, 2016, Ponemon Institute*

computer systems and would only agree to release control after a ransom, reported to be in the $15-20,000 range, had been paid in bitcoins. As in most ransomware situations, the dollar amount demand was low in comparison to the potential exposure from non-compliance. The demand in such cases is set intentionally low to encourage prompt compliance. In many instances, the perpetrator does not later come back to make a second attempt once a demand is paid. Perhaps that's honor among thieves; more likely it's a case of not wanting to test their luck twice on the same victim, who undoubtedly reported the incident to law enforcement. That's not always the case, though. Kansas Heart Hospital in Wichita, KS paid the criminal's initial demand, but the perpetrator came back and required a second payment. There have also been events where data was encrypted, the ransom was paid and the key needed to unencrypt the data was never provided.

Negligence / Human Error

Negligence, typically carelessness or simple human error, is often a major component of a breach. The United States Computer Emergency Readiness Team, a division of Homeland Security, estimated that as many as 85% of attacks could have been prevented by deploying software updates and patches provided by the manufacturer of the product. While this would seem to be a pretty straightforward issue to address, networks have grown significantly in size with new networked devices being added regularly, and each device has its own set of updates and patches.

Also last year, hackers reportedly exploited a known weakness in widely used software code (JBOSS) to breach Medstar, a large healthcare network. If the reports were correct, Medstar could have prevented that exploit by deploying a vendor-provided update or by deleting two lines of code. Warnings on the vulnerability were issued initially in 2007 and again in 2010, so this was neither a case of simply missing an update nor being exposed for a short time window.

Simple human error can have major consequences. A former patient at St. Joseph Health System (SJHS) in California did an online search and discovered that its patient records were viewable online due to an improper security setting on its network. A class action lawsuit was filed that resulted in a settlement agreement that could cost the system as much as $35 million. That settlement breaks down as follows: $7.5 million to plaintiffs, the largest settlement on a per plaintiff basis to date; $4.5 million for credit monitoring; $3 million to compensate for identity theft losses; $7.4 million for attorney fees and $13 million for improvements to bring SJHS into compliance.

Phishing

Phishing is a socially-engineered attack where system users are sent a spoofed e-mail made to look like it comes from a recognized or trusted source. The goal is to get the user to provide personal

(continued)

information and/or click on a link that deploys malware onto that user's network. The criminals cast a broad net by sending out thousands of e-mails figuring they will get some people to bite. Similar to a direct-mail advertising campaign, the anticipated uptake rate is of the traditional phishing technique. In contrast to a broad distribution, it is very focused and tactical, typically targeting primarily the executive suite of an organization. The criminal will initiate a request that appears to come from an executive in the organization to another employee who the attacker believes will have the authorization to make a large payment, transfer funds, approve an invoice or supply the desired information. The criminal makes it appear that the spear phishing email is coming from the CEO, CFO, COO or HR Director—people who typically would have the authority to make the request. The perpetrator hopes that the employee receiving the phony e-mail will think that it is coming from a peer or superior and will comply and deliver the goods, without question. Sophisticated hackers do their homework following executives on social media, perhaps hacking e-mail accounts to gain access to travel schedules. They spend significant amounts of time learning about the target, their interests, habits and routines in order to make their request appear as if it is legitimate. All it takes to derail such an attack is a phone call or a planned procedure that would not be known to a criminal.

Last year, a healthcare system HR employee was duped by a spear phisher posing as a senior finance executive into providing over 5,000 employee W-2s. The employee was so focused on pleasing the senior executive that the employee didn't bother to ask what it was for, why it was needed and whether that individual had the authority to request such information.

Distributed Denial of Service attacks (DDoS) are assaults on a network where the perpetrator uses computing power to flood the target's servers with more traffic than the network can handle, causing it to slow severely or completely shut down. Typically a DDoS doesn't involve disclosure of information, unless it is being used to distract IT security while another area of the network is being accessed. DDoS attacks can be financially oriented or intended to punish. The frequency of such attacks is on the rise in healthcare; however, these types of incidents are not as widely reported as breaches. There was a widely published DDoS attack in 2014 at Boston Children's, which was perpetrated by the hacker group Anonymous. It appears the hackers were most interested in making the point that it could be done.

There is growing concern over the ability to hack into medical devices that are connected to the internet. The closest known event to date was the extortion attack on Hollywood Presbyterian that impacted the facility's ability to interact with hospital equipment in the course of providing care. The attack did not specifically target individual medical devices, but it was ominous nonetheless. As part of a study on the issue, a researcher with Kapersky Labs was able to easily and successfully access an MRI machine to obtain access to medical records via a security vulnerability in the hospital's WiFi network. The possibility of a hacker being able to alter medical records to create false positive or false negative results, enter data that could alter the course of treatment, or even to control a device administering treatment is truly frightening.

Safeguarding Against Attacks

What can providers do? Based on the Kapersky researcher's experience we can draw a couple of conclusions:

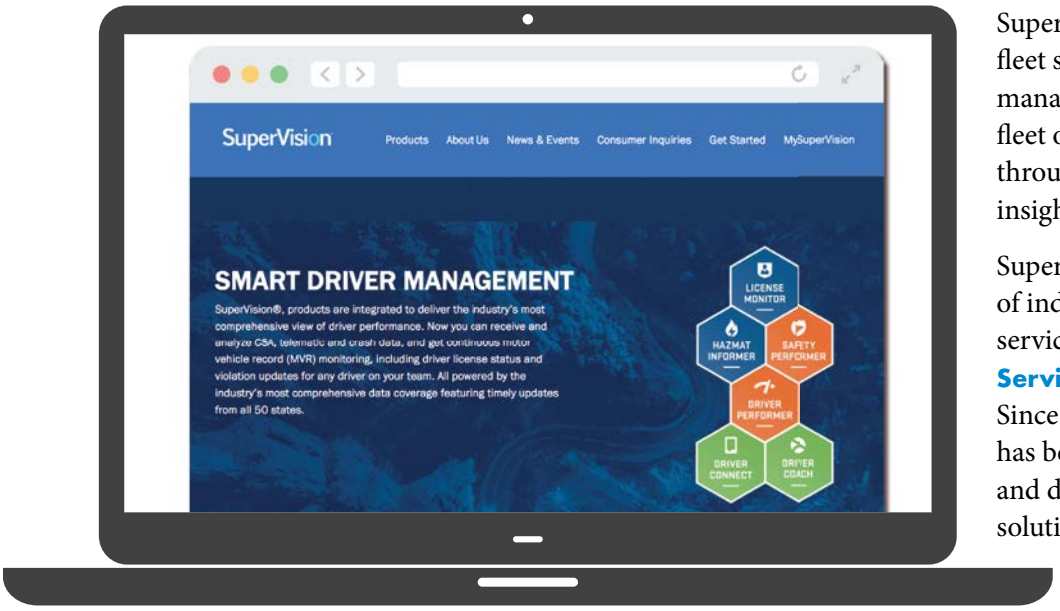
- It is vital to keep your networks and devices updated. The researcher got in by exploiting a flaw in the WiFi network's security settings. Updates are important!
- Use caution when choosing devices. The researcher also noted that some device manufacturers do an excellent job of securing their devices, while others, in a rush to meet functional needs, place security as a second- or third-tier priority in development. This problem is commonplace in the development of most mobile device applications, but one would hope that we could expect a higher emphasis on security in medical devices. One explanation for why that may not be the case is that many OEMs are not considered covered entities under HIPAA and therefore are not required to adhere to the same stringent guidelines as care providers. That puts device manufacturers and providers at odds. Inclusion of internet-connected security evaluation criteria to all medical devices is a possible means of mitigating a device hack. It is certainly not a guarantee, but if security is part of the decision-making process when the devices are procured, it would stand to reason that the likelihood of a hack would be decreased. Only time will tell.

Future articles include:

- **Part Three: Limiting Exposure through Preventive Measures**
- **Part Four: Preparing for the Time When Preventive Measures Fail**

New Vendor Discount Program: SuperVision

Napa River Insurance Services, Inc. is pleased to announce a new vendor discount program with SuperVision®.



SuperVision provides comprehensive, fleet safety and performance management solutions that optimize fleet oversight and driver behavior through advanced data, actionable insights, analytics, and reporting.

SuperVision is the latest in a line of industry-leading products and services created by **Explore Information Services** and **Solera Companies**. Since 1989, Explore Information Services has been providing risk data services and developing superior information solutions for commercial fleets, insurance companies, and government entities.

As our client, you will receive access to customized reports, as well as all of the other benefits offered by SuperVision, including:

- **Alerts** about any driver violations, suspensions or revocations
- **Alerts** when a license is expired, suspended, revoked or canceled, and when the status changes
- **Alerts** when a license is suspended for a non-moving violation, such as unpaid child support
- Motor vehicle record (MVR) **updates**, plus MVR reviews and automation
- Driver **violations** by geography, time frame and business unit
- **24/7 access** from any internet-connected device

We encourage you to contact your Napa River risk representative to learn more about the Napa River discount. To learn more about SuperVision, visit **eSuperVision.com**.

* *While neither Hudson Insurance Group nor Napa River Insurance Services, Inc. formally endorse any products, we do try to find proven industry vendors from which to secure product discounts for our customer partners.*

SuperVision is a registered trademark of Explore Information Systems, A Solera Company, Eagan, MN.

Wearable Technology Devices in Personal Injury Cases: Defense

Sadie A. Horner
Associate
The Bassett Firm

Wearable technology usage is on the rise. Today, "one in six consumers in the United States currently uses wearable technology."[1] Devices such as Fitbit® activity trackers, MicrosoftTM Band, and Apple Watch® have technology capable of tracking an individual's daily physical activity.[2] Wearable technology can be thought of "as partial witnesses, ones that carry their own affordances and biases."[3] The data that is collected from these devices can be used in a lawsuit for either a plaintiff or a defendant. Due to the growing popularity of wearable technology and its data collection capabilities, attorneys should begin utilizing these devices to prove or deny damages in personal injury lawsuits. In this article, we will focus on the defense in such cases.

Consider this hypothetical: a plaintiff has been involved in a car accident and is claiming that he is no longer capable of performing the physical activities he once did. Does the plaintiff have a Fitbit account or similar application? Does the Fitbit or similar device show any change in activity levels before and after the accident? The absence of such changes could significantly undermine the credibility of the plaintiff's claim.

Michael H. Bassett
Senior Partner
The Bassett Firm

But how do you get this information? Ask for it in written discovery requests and inquire about it at the deposition. Anticipate objections and be prepared to explain the relevance of the information contained within any "wearable technology devices" utilized by the plaintiff.

You may also be wondering: can discovery of this information be curtailed by Health Insurance Portability and Accountability Act (HIPPA) concerns? Unfortunately, there is no clear-cut answer. HIPPA is only applicable to covered entities and their business associates.[4] Wearable technology devices, such as those described above, could be considered "covered entities" cited in the statute. Additionally, since these devices must be registered with the entity before the data can be collected and analyzed for medical purposes, wearable technology devices may be considered "business associates" of medical entities covered by HIPPA. However, the information generated through fitness trackers, smartphones and mobile applications is generally not covered by HIPAA regulations. Thus, the defendant should, in most cases, subpoena the records with the pertinent data from the wearable technology device company.

(continued)

[1] *Piwek L, Ellis DA, Andrews S, Joinson A (2016) The Rise of Consumer Health Wearables: Promises and Barriers. PLoS Med 13: e1001953 doi. Available at: 10.1371/journal.pmed.1001953*

[2] *Kate Crawford, When Fitbit is the Expert Witness, ATLANTIC (Nov. 19, 2014), Available at: http://theatln.tc/22fb92A.*

[3] *Id.*

[4] *See, The HIPAA Privacy Rule, 45 C.F.R. Sect. 160.102*

However, there are a few steps that need to be taken before the data obtained from wearable technology can be used at trial. In order to be admitted at trial as evidence, such data must be authenticated. Since wearable technology devices are connected to servers, they can easily be manipulated; thus, savvy plaintiffs may argue the information is unreliable and inadmissible.

Courts have uniformly held that existing rules of evidence are "generally 'adequate to the task'" of authenticating electronic information and have declined to create new and special rules.[5] In other words, existing Rule 901 of the Texas Rules of Evidence governs the authentication of information obtained from wearable technology. To meet the requirements under this Rule, the defendant should have a third-party service or expert collect and analyze the data in order to present evidence sufficient to support a finding that the evidence is what the defendant claims it to be in compliance with the Texas Rule of Evidence Rule 901(a).[6] Consult with a data retrieval specialist for more information about the processes available for retrieving such information, along with the metadata to ensure accurate results.

In conclusion, wearable technology devices are increasingly present in today's society. Using this technology to rebut a plaintiff's damage claims is an innovative technique of which defense attorneys must be aware, and they should be prepared both to collect and to utilize this potentially invaluable information.

Fitbit activity trackers is a registered trademark of Fitbit, Inc. and/or its affiliates in the United States and other countries.

Microsoft is a trademark of Microsoft Corporation, Redmond, Washington. This article is an independent publication and is neither affiliated with, nor authorized, sponsored or approved by, Microsoft Corporation.

Apple and Apple Watch are registered trademarks of Apple, Inc., Cupertino, California. This article is an independent publication and has not been authorized, sponsored or approved by Apple, Inc.

[5] *Tienda v. State, 358 S.W.3d 633, 638-39 (Tex. Crim. App. 2012).*

[6] *See, TEX. R. EVID. 901(a)*

Now Is the Time for ELDs

Jeffrey K. Davis
Vice President of Safety
Napa River Insurance Services
317.810.2034
jdavis@napariverinsurance.com

After much speculation and debate, the mandate of Electronic Logging Devices (ELDs) becomes reality on December 18, 2017. As of this writing, there was nothing pending in Washington to delay the effective date of the ELD rule. The last attempt to do just that failed to pass in the U.S. House of Representatives in early September.

Contrary to popular belief, the Federal Motor Carrier Safety Administration (FMCSA) is ready to enforce the ELD mandate. Violations will be recorded and citations could be issued beginning December 18, at the local jurisdiction's discretion. However, the Commercial Vehicle Safety Alliance, in cooperation with the FMCSA, announced on August 28, 2017 that drivers of applicable vehicles that do not yet have an ELD will not be placed out of service until April 1, 2018.

The following are exemptions to the mandate:

- Drivers who currently use paper Record of Duty Status (RODS) for not more than 8 days out of every 30-day period
- Drivers who are required to keep RODS not more than 8 days within any 30-day period
- Drivers who conduct drive-away-tow-away operations, where the vehicle being driven is the commodity being delivered, or the vehicle being transported is a motor home or a recreation vehicle trailer with one or more sets of wheels on the surface of the roadway
- Drivers of vehicles manufactured before the model year 2000 (as reflected on the vehicle registration)

While these exemptions are available, a company may, of course, choose to proceed with an ELD in the aforementioned cases.

We have found that even the harshest critics of the mandate have become supporters, since this mandate makes compliance with the Hours of Service rules so much easier for the driver. ELDs also benefit the company by providing more accurate and timely information, resulting in more efficient dispatch of drivers. In many cases, fleet utilization has actually improved. Additionally, shipper/consignee activity, such as detention and other delays, can be better tracked and documented. Many carriers are already using this data to improve the work environment for drivers.

As with any new rule, there will be ongoing interpretation, and the anticipated change can oftentimes seem more difficult than reality. The reality is that, in the end, the ELD mandate will be good for safety and operations. Therefore, you should embrace the change and learn how to prosper from it.

The Napa River Risk Services team will help you in this task. We are available to work with you to help turn this new mandate into an opportunity for your organization. Meanwhile, you can stay up to date on the mandate at https://www.fmcsa.dot.gov/faq.

NAPA RIVER
INSURANCE SERVICES®

The information contained in this publication is provided for informational purposes only and is not provided as a substitute for advice from legal counsel regarding the content or interpretation of any law, regulation or rule. The information provided shall not revise, supplement or alter an insurance policy in any manner, nor is it intended as a substitute for advice from a risk management expert or legal counsel you may retain for your own purposes.

www.napariverinsurance.com