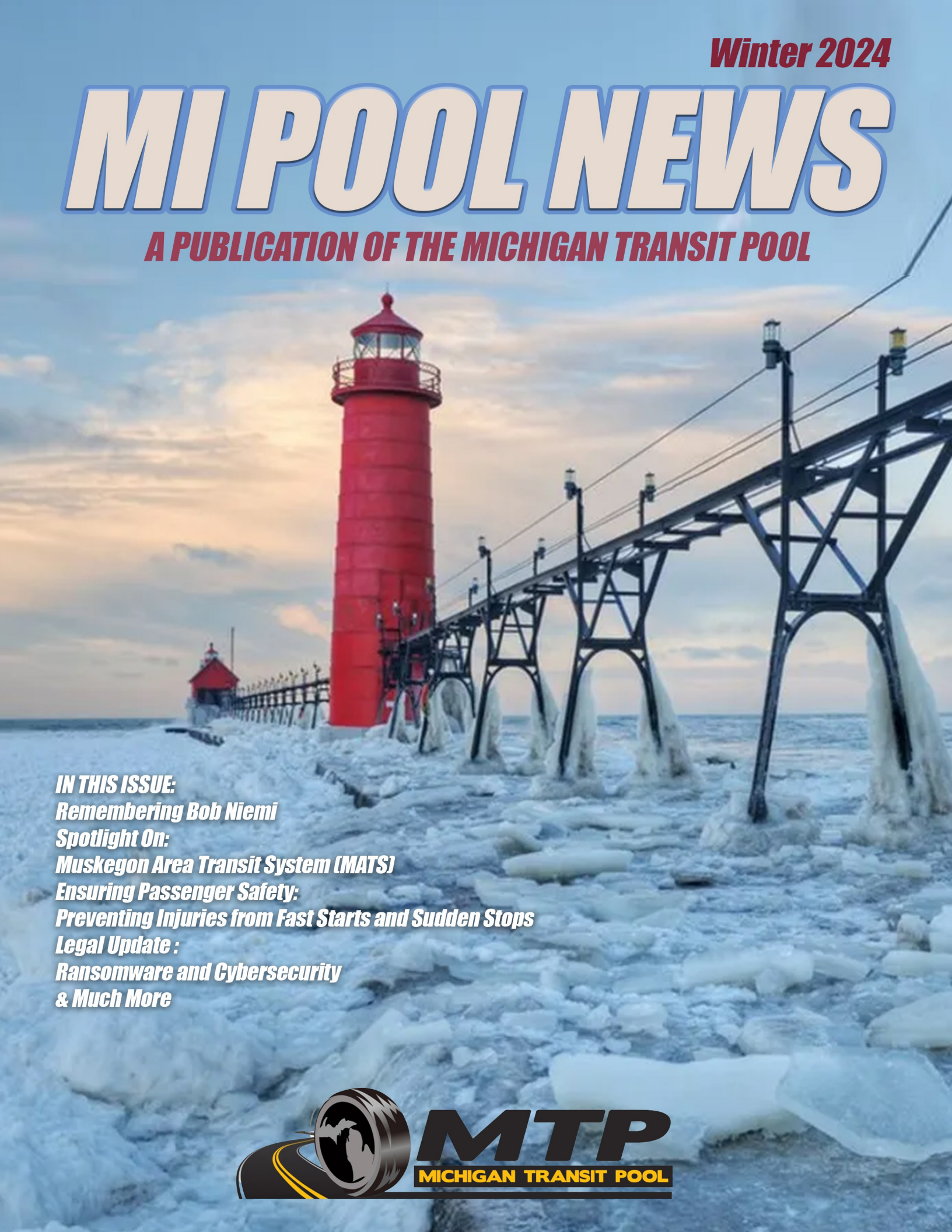
Winter 2024

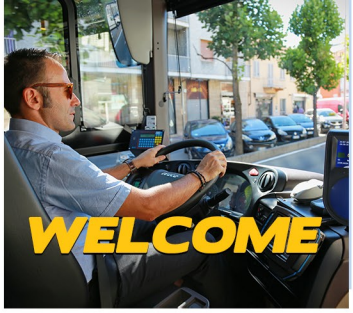
MI POOL NEWS

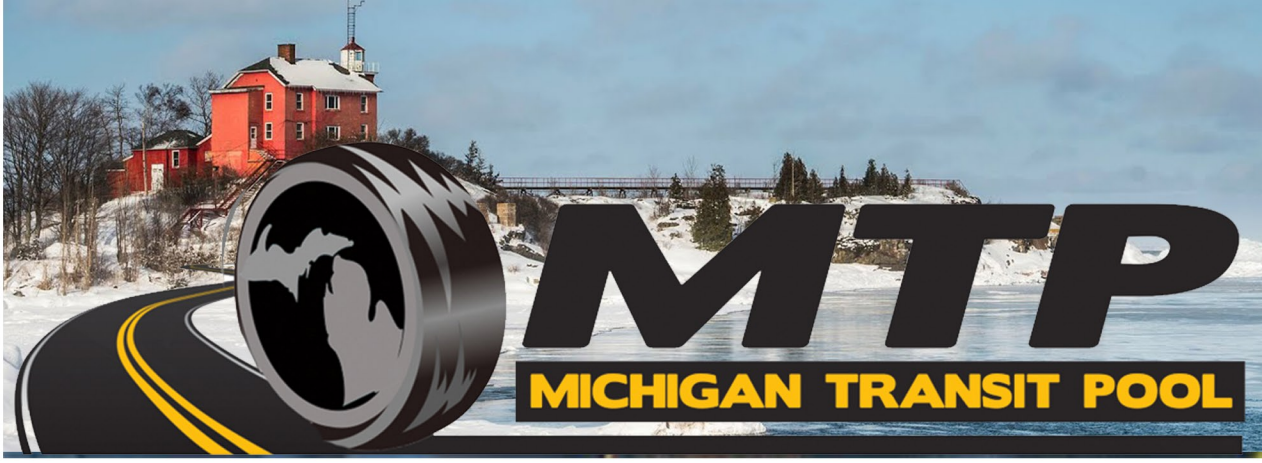
A PUBLICATION OF THE MICHIGAN TRANSIT POOL



IN THIS ISSUE:
Remembering Bob Niemi
Spotlight On:
Muskegon Area Transit System (MATS)
Ensuring Passenger Safety:
Preventing Injuries from Fast Starts and Sudden Stops
Legal Update :
Ransomware and Cybersecurity
& Much More

MTP
MICHIGAN TRANSIT POOL





Michigan Transit Pool Executive Committee

Dave McElroy
President

Larry Alpert
Vice President

Jim Oliver
Treasurer

Kelly Bales
Secretary

Tom Pirnstill

Karen Mendham

Mike Brown

Ken Jimkoski

Carrie Thompson

Joe DeKoning
TRL Liaison

Your ASU Team:
Glen Griffin

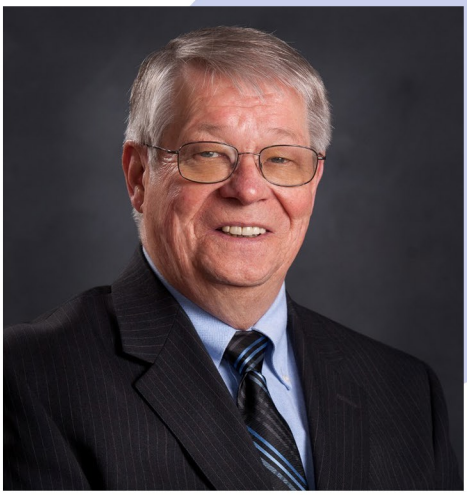
Kimberlee Hanes

Kristine Schreiber

Adam Wilberding

Wishing you a joyful and prosperous New Year!

May the coming year bring you happiness, good health, and new opportunities for success and growth. May you all have a great 2024! Happy New Year!



On a sad note, many of you may already be aware that **Bob Niemi** passed away on December 2, 2023. Bob provided 30+ years of service to MTP as a founding member who later served as President and Executive Director while becoming a friend to all of us. In addition, he was also the Executive Director of Marq-Tran, served as the Mayor of Marquette, and many other important community roles. Bob played an integral role in the formation of and provided guidance and direction to the Michigan Transit Pool that we know today.
MTP honored Bob's memory and extended condolences to his wife Joy and family.

We just came through the year end policy renewal period and anticipated possible rate increases, but we were fortunate to experience only a minor increase in the required Statutory Aggregate Insolvency Policy. Brokers indicated this slight increase was less than what was expected from the markets, and it was communicated to us that the lesser increase was due to the strong history of MTP. Kudos to all of the members in your efforts to reduce claims!

Save the date for the MTP Annual Meeting!! May 14th and 15th, 2024
We're moving NORTH this year and are attempting to finalize accommodations at Shanty Creek Resort in Bellaire, Michigan in Antrim County. More details to follow.

this publication powered by The ASU Group
Employee Owned • Client Focused

Spotlight on: MATS

Muskegon Area Transit System

MUSKEGON AREA TRANSIT SYSTEM
50 Years
1974-2024

The Muskegon Area Transit System (MATS) is a small urban transit system operating seven (7) fixed routes, ADA complementary paratransit, and on-demand microtransit services in the urban portions of Muskegon County. While operating as a department of the County of Muskegon, MATS does not receive County general funds, but rather relies on available federal and state grants, passenger fares, and modest match fund contributions from partnering local municipalities. MATS and its local partners are actively exploring the transition to an Act 196 Authority in the coming year, with the potential to bring additional local resources to the program.

Since 2019, MATS has made significant changes to its public transit offerings. Routes were realigned and reduced to address budgetary pressures. County-wide demand-response services that had no local funding source were ended and re-purposed to meet ADA Complementary Paratransit needs in the urban core only. And, while those services were reduced, MATS was among the first systems in the State to launch a turnkey on-demand microtransit service to fill in transportation gaps. Operated as a turnkey service by third-party contractor Via, the "Go2" service provides a new tech-enabled on-demand transportation option that has been very successful in meeting community needs and attracting passengers to a new model of public transportation. By deploying its Go2 program, MATS actually increased its daily service hours and geographic service area for general public riders.

Formed in February 1974, MATS will soon be celebrating its 50th Anniversary. For many of those years, MATS has participated in the Michigan Transit Pool's Liability Trust Fund, keeping its liability insurance costs stable and ensuring that the best practices that reduce risk can result in the return of premium dollars.

MTP Risk Management

Adam Wilberding

Ensuring Passenger Safety: Preventing Injuries from Fast Starts and Sudden Stops

Introduction:

Passenger safety is a paramount concern, and while buses are generally considered a safe mode of travel, the risk of injuries arising from fast starts and sudden stops cannot be ignored. The jolts and jerks experienced during these maneuvers can lead to a range of injuries among passengers. This article explores the importance of preventing such incidents and suggests measures to enhance safety on passenger buses.

The Impact of Fast Starts and Sudden Stops:

Fast starts and sudden stops are inherent aspects of bus travel, influenced by various factors such as traffic conditions, driver behavior, and the design of the road network. While these maneuvers may seem routine to seasoned passengers, they pose a significant risk to passenger safety. Common injuries resulting from abrupt movements include sprains, strains, whiplash, and even more severe injuries in some cases. Vulnerable passengers, such as the elderly and children, are particularly at risk, and preventing these incidents is crucial for fostering a secure and comfortable public transportation experience.

Driver Training and Education:

A fundamental step in preventing injuries from fast starts and sudden stops is comprehensive training and education for bus drivers. Drivers should be well-versed in the importance of smooth acceleration and deceleration, understanding the direct impact on passenger safety. Training programs should emphasize the significance of gradual speed changes, with a focus on anticipating traffic conditions to ensure a smoother ride. For example, TAPTCO provides hazard mitigation practices such as leave room (at least four seconds of following distance), look ahead, look around, focus on driving, and so on. Both classroom and behind the wheel instruction combined with periodic supervisory check rides help to ensure formation of critical driving habits. Additionally, educating drivers on the potential consequences of abrupt movements will heighten their awareness and commitment to safety.

Please consider attending one or more of the **Risk Management Subcommittee Meetings,** which are scheduled for the following dates from 9:00am to 10:30am.

January 8 • March 11 • May 13 • July 8 • September 9 • November 11

Both in-person and virtual attendance options are available. We value your input!

Technological Solutions:

Advancements in technology offer promising solutions to address the issue of passenger injuries on buses. The integration of advanced braking systems, accelerometers, and sensors can contribute to a more controlled and predictable driving experience. Automatic systems that regulate acceleration and deceleration can assist drivers in maintaining a smoother ride, reducing the likelihood of sudden jolts. The combination of advanced braking systems, predictive analytics, and collision avoidance technologies helps address the challenges associated with fast starts and sudden stops, ultimately reducing the risk of passenger injuries on buses. Fleet operators should explore these technological innovations and invest in systems that prioritize passenger safety.

Infrastructure Improvements:

Collaboration between transportation authorities and urban planners is crucial to creating road infrastructure that minimizes the impact of fast starts and sudden stops on buses. Designing roads with gradual slopes and dedicated bus lanes can facilitate smoother acceleration and deceleration. Additionally, the implementation of traffic management systems that prioritize public transport can help reduce congestion and enhance the overall safety of bus travel. Collaboration can lead to significant, long-term improvements.

Passenger Awareness:

Passenger education plays a pivotal role in preventing injuries caused by sudden movements on buses. Informative campaigns (e.g., PSAs, social media campaigns, informational brochures, etc.) and signage within buses can educate passengers on the importance of holding onto handrails, choosing secure seating, and being prepared for sudden stops. Use of visual aids, icons, and simple language helps to convey the message to a diverse audience. Installation of digital displays inside buses can periodically highlight safety messages and tips.

Automated announcements or recorded messages remind passengers about the importance of stability during transit. Communication that is repeated regularly will help to reinforce the safety message. Also, encouraging passengers to report incidents of erratic driving can also contribute to maintaining a culture of safety within the public transportation syste

Conclusion:

Ensuring passenger safety on buses demands an integrated approach that combines driver training, technological advancements, infrastructure improvements, and passenger awareness. By addressing the root causes of injuries resulting from fast starts and sudden stops, we can create a safer and more reliable public transportation system. It is a shared responsibility that requires collaboration between transportation authorities, bus operators, and passengers to foster an environment where everyone can travel comfortably and securely.

Legal Update on Ransomware and Cybersecurity

by David Klevorn
Murphy & Spagnuolo, P.C.
additional contributions by Andrew Zienty, law clerk

After a decline in ransomware attack rates in 2022, there was a recent uptick in ransomware and other cybersecurity attacks in 2023 – as MTP members are likely well aware given the recent attack on a member.

For those unfamiliar with ransomware, the Michigan Penal Code defines ransomware as a computer or data contaminant, encryption, or locks placed onto a computer system or network that restricts access by the authorized persons to those computers. The hackers who place the ransomware software, encryptions, or locks onto the computers can then demand the authorized persons who own the computer systems to pay money or other consideration (oftentimes in the form of an untraceable cryptocurrency) in exchange for the keys to unlock or remove the ransomware and restore proper access and use of the computers – i.e., holding a computer system and/or its data captive and locking out the authorized user until a ransom is paid.

The Federal Government agency set up to fight cyber-attacks – the Cybersecurity and Infrastructure Security Agency (CISA) – has published a guidance article on best practices for organizations to prepare for, prevent, and mitigate ransomware attacks. Available at https://www.cisa.gov/stopransomware/ransomware-guide
Some of the best practices that can be implemented are as follows:

(1) Maintain offline, encrypted backups of critical data;
a.Maintain and regularly update golden images of critical systems and retain backup hardware to rebuild systems if rebuilding the primary system is not preferred. Also, consider using a multi-cloud solution.
(2) Create, maintain, and regularly exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures;
a.Ensure notification procedures adhere to applicable state law (Mich. Comp. Laws Sections 445.63, 445.72).
(3) Implement zero trust architecture to prevent unauthorized access to data and services.
a.This means implementing a system that assumes a network is compromised and provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per request access decisions in information systems and services.

Some additional best practices for preventing and mitigating ransomware and data extortion according to CISA includes:

(1) Do not expose services, such as remote desktop protocol, on the web;
(2) Conduct regular vulnerability scanning to identify and address vulnerabilities;
(3) Regularly patch and update software and operating systems to the latest available versions;
(4) Ensure all on-premises, cloud services, mobile, and personal devices are properly configured and security features are enabled;
(5) Limit the use of remote desktop protocol and other remote desktop services and use a secure VPN if necessary;
(6) Implement phishing-resistant multi-factor authentication for all services (particularly email, VPNs, and accounts that access critical systems);
(7) Additional guidance can be found on the linked CISA article above
Another part of dealing with ransomware is the reporting of ransomware attacks to the proper law enforcement agencies. Many law enforcement agencies have specialized resources that provide guidance around ransomware attacks or have encryption keys if this particular ransomware has been combatted previously.

Legal Update on Ransomware and Cybersecurity

by David Klevorn
Murphy & Spagnuolo, P.C.
additional contributions by Andrew Zienty, law clerk

Once a system is compromised and ransomware is in a particular system, law enforcement can help with coming up with an action plan to address the data breaches and ongoing threats. It is worth assessing the data compromised and the demands made on a case-by-case basis, as reports indicate that only 13% of organizations who reported suffering a successful ransomware attack were able to successfully maneuver not just paying the ransom in 2022.

In that regard, reaching out to your attorney early on in the process can be vital because of the notice and reporting conditions required under state and federal law and the fact that communications soliciting legal advice on these topics is privileged and protected and not subject to production under the Freedom of Information Act.

For both Michigan and Federal Law on the topic of cybersecurity, the law does not require perfection, just that there are "reasonable precautions" to protect consumers' personal information. If a data breach does occur that causes "substantial loss or injury" to a Michigan resident, then MCL 445.72 requires that Notice be provided to the impacted resident "without unreasonable delay." The Michigan Notice of Security Breach statute provides for the opportunity for breached companies to measure the scope of the breach and restore reasonable integrity to the system, but after the above is accomplished, then the law requires notice to be provided to impacted residents unless law enforcement indicates that providing notice may impede their ongoing investigation or jeopardize national security.

Ideally, transit authorities can be proactive with some of the guidance provided by CISA. However, in this day and age, breaches inevitably may occur and so members ought to be prepared with response plans with contingencies of how to act when faced with a cybersecurity threat. As indicated above, involving law enforcement and legal counsel can help in several aspects in that regard both during and after a cyberattack. This area is constantly changing so staying up to date on changes and advancements is crucial.

The general information provided in the above article in no way constitutes legal advice as every situation is different. MTP members should consult with their attorneys for specific guidance.