FROM THE DESK *of*

Trey Boudreaux, *LASERS Executive Director*

> *"We appreciate your trust in us and will continue to work tirelessly to maintain it."*

HOW LASERS PROTECTS YOUR PERSONAL DATA

I would like to start my first letter in *The Beam* by expressing that I am humbled and honored for the opportunity to lead the retirement system I've been a part of for 32 years. I was fortunate to work with Cindy Rougeou throughout my 15-year tenure at LASERS and I am excited to work with the wonderful team currently assembled. Cindy set the best example of upholding the LASERS mission to provide a sound retirement plan for our members, and the standard of her fearless leadership will continue.

As executive director, I intend to continue operating LASERS transparently while promoting our outreach efforts. I invite you to stay informed about your System by visiting our website at *www.lasersonline.org*, attending seminars, creating a myLASERS account, and signing up for *Member Connection* emails.

Cybersecurity and the security and protection of your personal data will remain a top priority. Considering the recent MOVEit data breach that impacted the Office of Motor Vehicles, it is an ideal time to reassure you about the rigorous measures LASERS has in place to protect your personal data.

The data breach was a large-scale cyberattack that placed the personal data of millions of individuals at risk of exposure to hackers. The attack was aimed at MOVEit, a file-transfer system trusted by various organizations worldwide, from government agencies to universities and multinational corporations, for the secure transmission of sensitive information.

While LASERS does not utilize MOVEit, we understand the magnitude of such incidents and recognize that our commitment to safeguarding confidential member information has never been more critical.

Here are some of the mechanisms in place at LASERS to help safeguard your data:

Limited Employee Access: At LASERS, member information is only accessible to employees with a legitimate business reason to access this information. Our 'least privilege' policy ensures minimal internal exposure of your personal data, minimizing the risk of internal breaches.

Data Encryption: We use a secure encryption process for all information transmitted to and from LASERS. This transforms your data into secure code that can only be interpreted by authorized systems, adding an essential layer of protection.

Frequent Security Audits and Assessments: LASERS regularly conducts internal and external audits to ensure our systems meet or exceed industry security standards. We continuously assess and improve security measures to keep up with evolving threats.

Employee Training: Our staff is our first line of defense. Every member of the LASERS team receives ongoing training in data security and privacy to ensure they are aware of best practices and emerging threats.

Advanced Security Measures: Our security measures include physical and technological tools designed to prevent unauthorized access to your information. We utilize state-of-the-art IT infrastructure designed to protect sensitive data. These measures include robust firewalls, anti-virus protection, and real-time monitoring of our systems. Our systems are regularly updated to keep them secure from the latest threats and vulnerabilities.

We encourage all of our members to practice personal data security as well. This includes regularly changing your passwords, avoiding suspicious emails or links, and monitoring your personal accounts for any irregular activity. *Nexsteps.la.gov* has proven to be a good resource for Louisiana residents to use following the data incident at the Office of Motor Vehicles.

LASERS is fully committed to protecting your information. We appreciate your trust in us and will continue to work tirelessly to maintain it. ■