VIEWS & VISIONS

A publication of Bowles Rice LLP

Summer 2015

Protecting the Information of Those Who Serve West Virginia

Jeffrey E. Fleck, Executive Director
West Virginia Consolidated Public Retirement Board

Jeffrey E. Fleck is the Executive Director of the West Virginia Consolidated Public Retirement Board (CPRB). The CPRB is the entity responsible for administering the State's nine retirement systems.

Mr. Fleck has been with the CPRB since February 2007, when he was hired as the Chief Compliance Officer. He became the Executive Director in October 2011.

Prior to employment with the State of West Virginia, Mr. Fleck spent the previous 15 years in the private sector, specifically in the health care industry. He held various roles at the former Putnam General Hospital in Hurricane, West Virginia and Pleasant Valley Hospital in Point Pleasant, West Virginia.

Mr. Fleck is a member of the National Association of State Retirement Administrators (NASRA) and the National Council on Teachers Retirement (NCTR). He also serves as a member of the West Virginia Municipal Pensions Oversight Board.

He received his master of business administration degree from the University of Charleston and earned his bachelor of science degree in communications from Liberty University.

"Serving Those Who Serve West Virginia." That is the motto of the West Virginia Consolidated Public Retirement Board (CPRB), and there are many ways that we accomplish this goal. Most notably is supplying a monthly annuity for over 60,000 retirees and administering the retirement plans of almost 80,000 active employees with a total of over $13 billion in assets. Of equal importance is the responsibility of protecting the Personally Identifiable Information (PII) of our customers.

As part of our service to members, retirees and employers across the state, the CPRB administers nine separate and unique retirement systems. The two largest are the Public Employees Retirement System and the Teachers Retirement System. Additional retirement systems include the Teacher's Defined Contribution Plan, Deputy Sheriff's Retirement System, State Trooper Plan A, State Trooper Plan B, Emergency Medical Service Retirement System, Judges Retirement System and the Municipal Police and Fire Retirement System.

The CPRB has embarked on a multi-year implementation of a new core pension processing system that will replace the current 30-year-old mainframe system. This project is known as COMPASS, and it will help transform the capabilities of CPRB. When fully implemented in 2017, the new COMPASS system will allow members and employers to perform many more activities over the internet. For instance, retirees will be able to manage their own beneficiary information and check deposit information. Active members will be able to apply for retirement at their own convenience from home, and employers will be able to manage the membership information, wage and service information electronically at any time.

These self-service and internet automation features will provide capabilities that customers are excited to have in order to help make the process of managing information much faster and easier for them. Enabling customers to access this information over the internet requires a greater level of technology and sophistication to ensure the security of customer information and data. This member information contains very sensitive and confidential data, such as social security numbers, account information and beneficiary information. So keeping this data secure, both through the course of the project, as well as for years to come, is a top priority for CPRB.

Some of the ways that the CPRB will protect the member and retiree information during the project include:

- **The use of 128- Bit Encryption.** This is an internet cryptography standard that applies to the methods used for transferring information. This type of encryption is generally known as "strong encryption," and it is implemented through specialized certificates.
- **The use of scrambled data during the construction and testing of the project.** This technique ensures that no actual member data is used while building the system. When working with the system, none of the developers have access to actual member information.

- **A Security Accreditation and Certification from the vendor, Deloitte LLP.** Deloitte is one of the largest and most respected system integrators in the world and, as part of this project, they will certify that the information is protected during the life of the project.
- **Network Vulnerability Assessments (NVA).** One of the highest levels of security assurance comes through hiring an independent internet security firm to actually attempt to "hack" into the system at multiple phases through the project. This is a best practice across industries that deal with the most sensitive information. Large banks and other financial institutions use this same strategy when deploying new software. At five distinct time periods throughout the life of the project, an independent firm hired by CPRB will attempt to penetrate the COMPASS system. Any vulnerability found will be addressed and remedied prior to the system going live.

Performing these steps during the project helps to ensure that no sensitive information can be accessed by unauthorized parties. But CPRB's commitment to security does not end there. Following the system implementation, security will remain a paramount concern. Some of the ways that CPRB will continue to protect member and retiree data indefinitely include:

- **The use of SSL Encryption for all external self-service environments.** When members, retirees and employers are accessing information over the Internet, they can be confident that encryption of the information is managed in secure ways.
- **Intrusion Detection.** The State of West Virginia utilizes specialized software to prevent and identify any intrusions on the state's network infrastructure. By housing the software on the state's secure infrastructure, the system is continuously managed 24 hours a day and seven days a week.
- **Discontinuing the use of Social Security numbers as the primary means of managing member information.** Migrating away from using Social Security numbers in favor of a randomly generated Member Account Number helps to protect PII well beyond the life of the project. This is another best practice that is used by large financial services organizations to ensure that even internal users and CPRB employees do not use sensitive information such as Social Security numbers during the performance of their duties.
- **Masking of information.** Masking is a technique whereby certain information on statements and correspondence is intentionally hidden with asterisks (*) and other characters to ensure that correspondence going out of the office is also devoid of sensitive information. Masking sensitive information on all communications such as correspondence and member statements helps to prevent anyone from gaining information, even through the mail system.

CPRB is committed to securing the sensitive information of all of its members and retirees. The techniques and strategies described above are some of the best practices in the industry. The COMPASS project enables faster and easier access for members, retirees and employers, but this will be balanced with the information security that is essential for providing reliable service. V