



## EJReynolds – Cybersecurity Commitment

### Trust your retirement plan development and your personal data with the experts at EJReynolds.

Retirement Plan Cybersecurity is now a top priority focus for the Securities & Exchange Commission (SEC) and the Department of Labor (DOL). In 2021, both agencies released guidelines and regulations addressing this important topic, and the trend will continue in the future. The DOL indicated that an audit program is forthcoming. For additional information on the DOL regulations, go to our website blog about cybersecurity and click on Department of Labor Issues Guidelines for ERISA Fiduciaries on Cybersecurity.

What can you do to ensure your data is safe? EJReynolds has taken definitive measures to safeguard our client information with our innovative cybersecurity commitment that will give you peace of mind knowing your most confidential information is safe and secure. Our advanced cybersecurity program stems from our core principles of trust, integrity, and ethics. We collect only the necessary information to consistently deliver the best products and services for our clients. All EJReynolds employees are required to complete ongoing extensive training programs on new threats and how to manage them. We have implemented security standards and processes to ensure that access to client information is limited to your EJReynolds Plan Consultant.

#### Our best practice cybersecurity protocols include:

##### - Citrix ShareFile© – secure file sharing

EJReynolds' secure file-sharing link provides a safe and secure way to transmit sensitive information online. This ensures that files are sent and received with bank-level encryption. You must register through ShareFile's one-time enrollment process to send and receive files securely. We are aware this may be an initial inconvenience, but we want our clients' information to remain protected.

##### - Two-factor authentication

EJReynolds has implemented a two-factor authentication process for our Plan Consultants to access the network environment. This practice, 2FA for short, is the most advanced form of security from any type of password-based attack. EJReynolds' employees must confirm a security code sent to an authenticator application when they log in every morning through another Cisco© product, Duo©. This process is implemented on the various applications that are used in our day-to-day administration of a plan, including our Customer Relationship Management (CRM) application, Government Forms, and Valuation System, even to open our email. You may already know, but the various investment platforms we work with have used this process for years.



WHERE IS YOUR COMFORT PLACE?  
EJR CAN HELP YOU GET THERE.

9050 Pines Blvd., Suite 202, Pembroke Pines, FL 33024

Office: 954.431.1774 Fax: 954.438.7250

[www.ejreynoldsinc.com](http://www.ejreynoldsinc.com)

### - Managed Detection & Response (MDR)

EJReynolds' Firewall Security system protects our computer network from being attacked by online hackers, worms, viruses, etc. It is designed to stop unauthorized access to the company's computer systems. Additionally, we have implemented an Application Control service that blocks the installation of any software on our workstations, unless specifically approved at the corporate level. MDR identifies indicators of compromise and isolates any affected computer. It uses Artificial Intelligence (AI) to watch what may be running on a computer. If suspicious behavior is detected, AI escalates the issue to a human IT manager, around the clock, 24/7, for review and if the behavior is related to a bad actor, the machine is quarantined from the network, limiting the scope of damage done.

### - Industry-leading Threat Phishing and Email Protection

Proofpoint Email Protection is the industry-leading email gateway. It uses Nexus AI, an advanced machine learning technology. Email Protection accurately classifies, detects, and blocks threats, such as business email compromises. It also provides advanced email filtering controls for phishing, spam, bulk graymail, and other unwanted email. This advanced threat protection helps to protect our organization from malicious attacks.

### - DNS Content Filtering

With staff working remotely and on the go these days, DNS Filtering provides web content filtering wherever staff are located. This helps web surfing on company-issued computers as well as provides web defense against malicious websites.

### - Dark Web Monitoring

Dark web monitoring provides around-the-clock monitoring and alerting for compromised digital credentials, scouring millions of sources, including botnets, criminal chat rooms, peer-to-peer networks, malicious websites, bulletin boards, and illegal market sites. All email addresses for EJReynolds' employees, including the personal accounts for certain officers and managers, are monitored on the "Dark Web" for breaches in security. We are notified immediately if these critical assets are compromised, affording the chance to secure them before they may be used for identity theft, data breaches, or other crimes.

### - Continuous training

Since 2017, all employees have been required to complete extensive training programs through KnowBe4.com®, a nationally recognized leader in security awareness training. Along with monthly training on the latest ERISA rules and regulations, each employee must complete training sessions in cybersecurity.

Hackers constantly change their tactics; EJReynolds is constantly training our staff to prepare for these situations.

Our commitment to your security is just one more reason to trust your retirement plan administration to EJReynolds. For our latest Cyber Security Updates, go to [www.ejreynoldsinc.com/cybersecurity](http://www.ejreynoldsinc.com/cybersecurity).



WHERE IS YOUR COMFORT PLACE?  
EJR CAN HELP YOU GET THERE.

9050 Pines Blvd., Suite 202, Pembroke Pines, FL 33024

Office: 954.431.1774 Fax: 954.438.7250

[www.ejreynoldsinc.com](http://www.ejreynoldsinc.com)