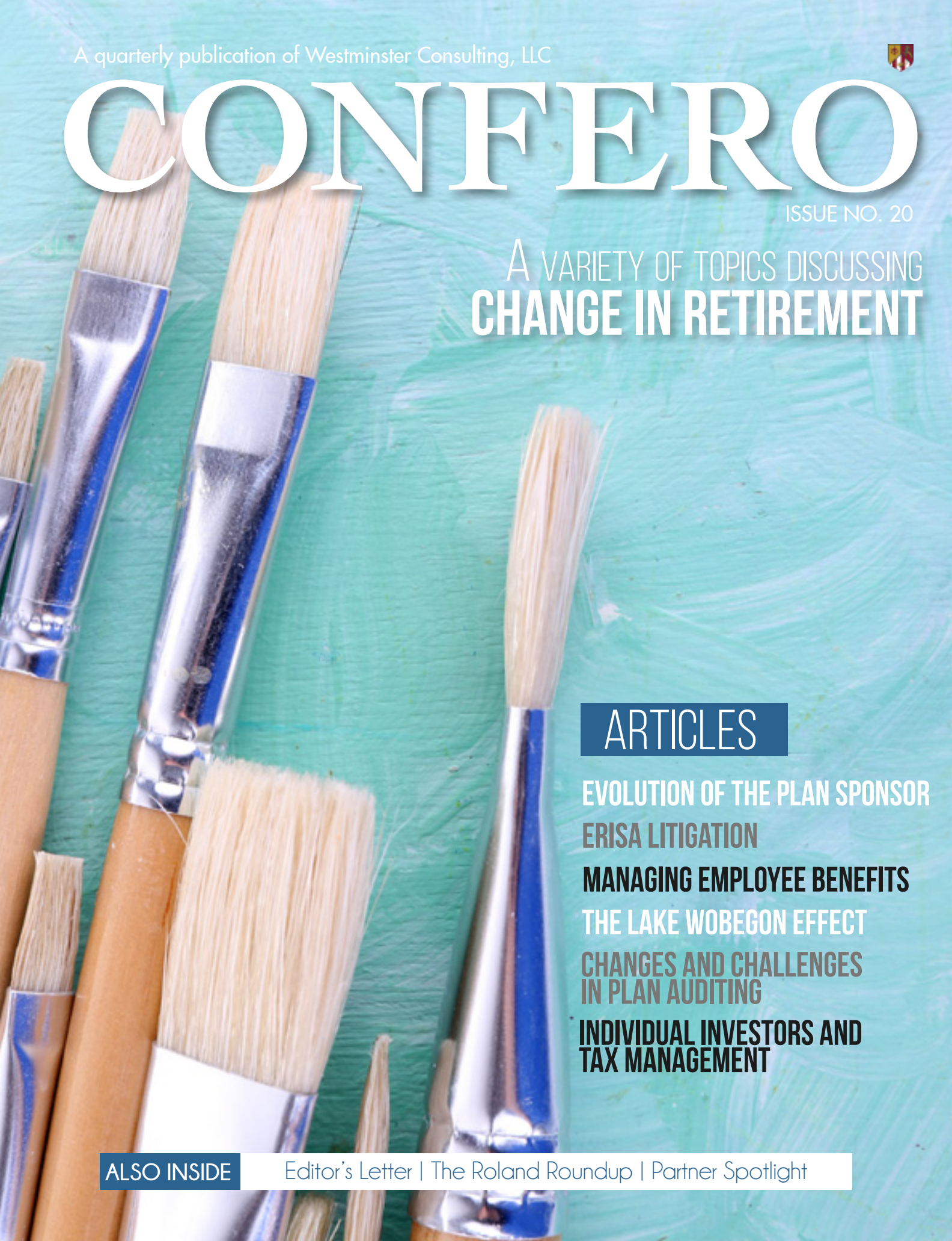
A quarterly publication of Westminster Consulting, LLC

CONFERO

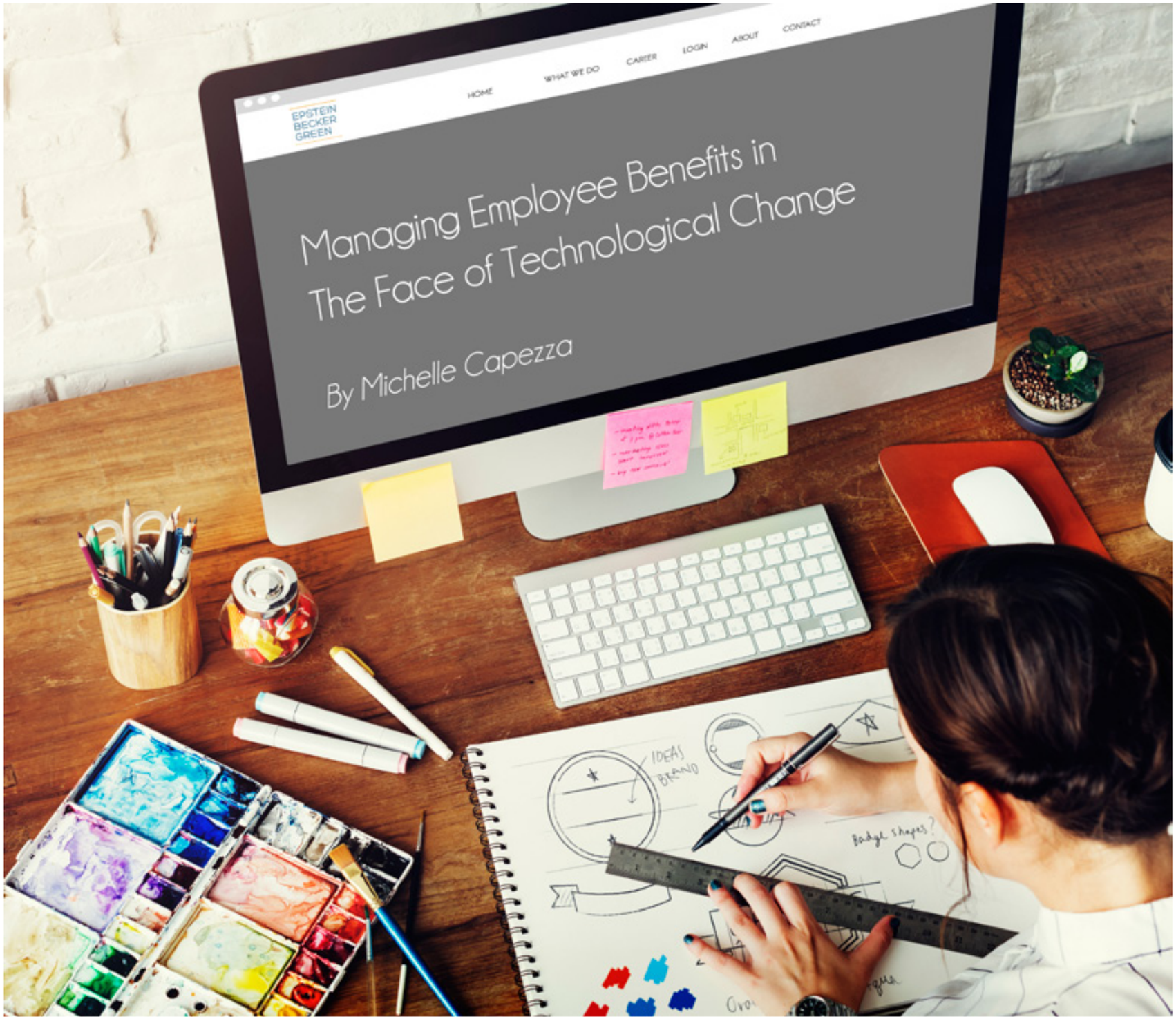
ISSUE NO. 20

A VARIETY OF TOPICS DISCUSSING CHANGE IN RETIREMENT



ARTICLES

ALSO INSIDE



There are many employee benefits challenges facing employers today, from determining the scope and scale of traditional benefits programs to offer that will attract, motivate and retain multigenerational employees, to embracing new models for defining and providing benefits, while simultaneously managing costs. In the midst of these challenges is the wave of technological change that is impacting all areas of the workplace, including human resources and benefits. In recent years, many new technological tools have emerged to aid in the administration of benefit plans, delivery of participation communications, as well as provide education and advice. These tools often require collection of sensitive data or allow employees to provide personal information in an interactive environment, such as:

- Benefits, HR and payroll software, and plan recordkeeping, systems
- Online and mobile applications for benefits enrollment and benefits selection assistance
- Social media tools and applications for benefits information and education
- Online investment allocation tools, robo advisors, financial platforms
- Telehealth and wellness programs

These and other advancements are a sign of the times. While they appeal to employees, reduce burdens on employers, and assist in driving down program costs, organizations must be mindful that cyberattacks on benefit plans and participant information have occurred and measures should be taken to protect against such data breaches.

The Advisory Council on Employee Welfare & Pension Benefit Plans (the "Council") began studying the importance of addressing privacy and security issues with respect to employee benefit plan administration in 2011 and provided a final report to the Secretary of Labor in November 2016 regarding cybersecurity considerations for benefit plans. The Council has raised concerns regarding potential breaches of the technological systems used in benefits administration, including the theft and misuse of personally identifiable information ("PII") and personal accounts. Organizations, and plan fiduciaries, should take the time to familiarize themselves with the issues in the Council's studies and reports and develop a policy for protecting PII and assets, especially when implementing and/or expanding the use of existing technological tools in the benefits area. Addressing these issues now will provide a solid foundation upon which to add new technological tools as they arise.

> The time is now to examine and address existing platforms and tools being used, identify potential risks, and implement action steps to improve practices and procedures.

What types of issues should be addressed in a Benefits Tech Policy?

- ***The Organization's Parameters and Vetting Process for Usage of Technological Tools Handling Sensitive Employee Data.*** When utilizing Benefits Tech tools which collect PII of employees using the tools, as well as personal health information (as applicable), extra steps should be taken to ensure protection of this information as it enters cyberspace. At the data level, consideration should be given to the kinds of data that will be collected, how it will be used and stored, encryption measures, and how any breach will be addressed and communicated, consistent with the organization's cybersecurity policies. Organizations should also establish parameters regarding how to maintain an inventory of all data collected by the various sources and tools to determine how to monitor the security of the data on an ongoing basis. Further, tools which apply to different benefits programs may require vetting through different channels. For example, if a group health plan-related tool is being considered, use of the tool may need to be coordinated with HIPAA privacy and security policies. If it is a retirement investment advice tool, plan fiduciaries should not only prudently select, and monitor, the robo advisor as an investment adviser, but also undertake due diligence of its PII privacy and security measures.

- ***Standards for Service Providers and Tech Tools.*** A Benefits Tech Policy can define the organization's protocols for review of any benefits technology service provider's service agreements, and product information, with risk management, IT, legal, and procurement areas. It can define the types of questions to ask service providers prior to engagement or upon renewal, such as confirmation of their cybersecurity program and certifications, details regarding how they handle, encrypt and protect data, data breach notification procedures, provision of reports regarding their controls, their levels of insurance and scope of their assumption of liabilities. It can also establish rules for any IT and security review of service provider systems, including requests for penetration tests to detect security risks. The goal of this type of effort should serve to confirm that the service provider, as well as the tool itself, meets the organization's cybersecurity risk management standards.

- ***Standards for Employees Establishing and Maintaining Use of the Benefits Tech Tools.*** Organizations should ensure that all personnel who have access to PII are properly trained in safeguarding it, including secure transmission of any data to third party service providers. Individuals should be designated to handle any benefits-related data breach response and have set procedures for reporting same through the appropriate channels of the organization. Organizations should take great care to ensure that internal personnel handling PII are also properly vetted and that measures are taken to protect against internal breach of PII security.

- ***Cybersecurity Insurance Requirements.*** Organizations are familiar with various types of insurance for their businesses including errors and omissions, criminal, and fiduciary liability insurance. Cybersecurity insurance has also emerged in recent years and can offer various types of coverage, including coverage that would allow a benefit plan to trigger coverage upon a breach for certain disaster recovery and response assistance. Organizations should assess their needs and gaps in existing coverage to ascertain how cybersecurity insurance can be obtained with appropriate levels of coverage which is specific to, and coordinated with any other policies to fit, their employee benefits needs.

- ***Plan Fiduciary Responsibility.*** Although the Council reports did not address whether cybersecurity is a fiduciary responsibility, plan fiduciaries should be mindful of their duties to carry out their responsibilities prudently and in the best interests of plan participants and beneficiaries. A Benefits Tech Policy which takes into account fiduciary responsibility, either separately or as part of one policy, can serve to outline the standards that plan fiduciaries should follow when handling participant data and/or delegating plan administration authority to individuals or third parties who will handle and transmit PII. It can also address any breach notification, participant communication and remediation measures. Further, it can set forth the organization's policies for indemnifying the plan fiduciaries for their actions so long as they did not act with gross negligence or with willful misconduct.

This list of issues is not exhaustive; organizations should identify where they may have risks and develop a policy that works for them. In this Digital Age and time of unprecedented change, the time is now to examine and address existing platforms and tools being used, identify potential risks, and implement action steps to improve practices and procedures. Development of a Benefits Tech policy, which takes into consideration organizational risk management perspectives and requirements for doing business with vendors, as well as plan fiduciary concerns, will enable employers to face these challenges head-on, improve the employee experience and reduce potential liabilities.

Michelle Capezza is an employee benefits and executive compensation attorney and a Member of EpsteinBeckerGreen, resident in their New York office.

She can be reached at mcapezza@ebglaw.com or 212-351-4774.

Confero Fall 2017: Change in Retirement
Used with permission of Westminster Consulting, LLC