INTERNATIONAL
PENSION LAWYER

U.S. Moves Towards National Data Privacy Framework

Kevin Walsh
Groom Law Group

kwalsh@groom.com
United States

Introduction

While the European Union led the world on data privacy through the enactment of the General Data Protection Regulation ("GDPR"), developments in the United States suggest that a similar data privacy regulatory structure may be forthcoming that will also affect pension and benefit plans and their service providers and advisors. This can be seen both through recent enforcement initiatives and through policy developments. First, in September 2018, the U.S. Securities and Exchange Commission ("SEC") announced that it had settled claims related to the cyber security policies and procedures to protect personally identifiable information ("PII") held by Voya Financial Advisors' (the "Advisor"), a registered investment advisor and broker-dealer. Second, the U.S. Congress and federal regulators have taken steps towards implementing a nationwide privacy framework. Both the enforcement initiative and policy developments are discussed below.

Enforcement Initiative

The SEC entered into a settlement decree with the Advisor that described how cyber criminals had impersonated the registered representatives of the Advisor by calling the Advisor's support line and requesting that they reset the registered representatives' passwords. Ultimately, through the resetting of passwords, intruders were able to gain access to the PII of over 5,000 of the Advisor's customers.

This was the first SEC settlement related to its Safeguards Rule and Identity Theft Red Flags Rule. The Safeguards Rule was enacted with the Gramm-Leach Bliley Act of 1999 and requires that investment advisers and broker dealers adopt written policies and procedures that address the protection of customer records and information. The Identity Theft Red Flags Rule requires that financial institutions develop and implement an identity theft program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of an account.

The settlement agreement described that the Advisor did not comply with the Safeguards Rule because its policies and procedures were not reasonably designed to protect customer information. Similarly, the settlement agreement described that the Advisor violated the Identity Theft Red Flags Rule because it had not updated its program since 2009 and failed to provide adequate training to its employees.

This settlement serves as a reminder to those in the retirement space that the world is evolving, and the risks associated with operating within the retirement space is changing as well. Moreover, U.S. regulators in this space are becoming much more sophisticated and interested in these issues as privacy and data breaches continue to make headlines. At a minimum, those in the retirement industry should review and update their data security policies and procedures as necessary and schedule regular updates to such policies to ensure that they stay current. Concerns surround not only the cybersecurity of the employers

and service providers, but how best to avoid cyber-theft from individual accounts. Those handling PII should also provide regular training to employees to ensure that the data security policies and procedures are properly implemented.

Data Privacy Policy Developments

In addition to enforcement action, both regulators and legislators have been actively working to modernize the United States' framework for personal data. This comes not only in reaction to GDPR, but also in response to a raft of state data and local privacy proposals. Earlier this year, California passed a data privacy statute based on GDPR. In addition, municipalities like Chicago and San Francisco are considering local ordinances. In the face of this fracturing regulatory landscape, leading technology companies and privacy advocates have been pushing for a uniform federal framework.

The Senate Committee on Commerce, Science, and Transportation (the "Commerce Committee") has held a number of hearings recently and is believed to be working on draft legislation. The Commerce Committee heard from a panel of executives from communications firms and tech companies and suggested that federal legislation may be forthcoming. Chairman John Thune (R. South Dakota) stated that "there is a strong desire by both Republicans and Democrats, and by both industry and public interest groups, to work in good faith to reach a consensus on a national consumer data privacy law." The Commerce Committee held a second hearing with testimony from privacy advocates, such as Andrea Jelenik, the head of GDPR enforcement. After these hearings, Chairman Thune has indicated that he is working on draft legislation. In addition, Senator Ron Wyden (D. Oregon) has introduced legislation.

In the House of Representatives, both parties have also indicated a desire to work together on data privacy legislation. Representative Greg Walden (R. Oregon 2), Chairman of the House Energy and Commerce Committee recently stated that, "now is the time to take action to better protect consumer privacy while still allowing for the incredible innovation that has made America's tech sector the envy of the world." On the Democrat side, Representative Ro Khanna (D. California 17) recently introduced a set of principles for an "Internet Bill of Rights".

Finally, U.S. federal regulators have not been waiting for Congressional action. The Federal Trade Commission is currently re-examining its approach to data privacy. In updating its 2012 guidance, it is holding hearings in December 2018 and February 2019 on data security and privacy. Simultaneously, the National Telecommunications and Information Administration, an organization within the Commerce Department, has put out a request for comment to develop the Administration's policies on data privacy with the aim of developing "ways to advance consumer privacy while protecting prosperity and innovation."

While it is unlikely that a data privacy law will be passed before the end of the current Congressional term (January 2019), it is likely that Congress remains focused on enacting a uniform federal standard and that regulators continue to refine their proposals to protect data of individuals broadly and plan participants in particular.

Conclusion

While data privacy had traditionally been seen as an area of concern primarily to technology companies, service providers who interact with U.S. retirement and health plans may want to watch the area closely. In providing services to a plan, a service provider may possess or process a significant quantity of personal data. As a result, it will be important to monitor U.S. developments in data privacy regulations, and in our increasingly globalized economy, how they will dovetail with privacy regulation from other jurisdictions such as the EU.