Raising the bar

Cybersecurity litigation and DOL guidance

Worldwide cybercrime cost more than $1 trillion in 2020.[1] And as technology to stop cybercriminals evolves, so do the criminals. It's vital to guard information against cybertheft.

Trending decisions

Court cases regarding cybercrime are becoming more common. Participants whose data is compromised or who have suffered monetary losses from cybercrime bring cases against plan sponsors and service providers alike. Who is responsible? The answer isn't always clear, but there are takeaways from recent case law and guidance from the U.S. Department of Labor (DOL).

Case examples

Let's look at the case law first.

- In Kimbriel v. ABB, employees' emails were hacked through a phishing scheme, resulting in the compromise of personally identifiable information associated with the plan. A class action suit was brought on behalf of the victims of the breach. The court dismissed the complaint because no actual damages occurred. The plaintiffs couldn't show that money was stolen based on the breach or that any would be stolen in the future. The court ruled there was not yet a case that could be brought in court.[2]
- In Leventhal v. M and Marblestone Group, a participant (who was a trustee/plan fiduciary) sued the TPA and plan custodian for allegedly failing to safeguard participant accounts after cybercriminals hacked a remote-working employee of the plan sponsor and got distribution forms. The criminals withdrew more than $400,000 from the plaintiff's account. The court denied the motion to dismiss, finding that the TPA and the custodian were fiduciaries for purposes of the plaintiff's claim. The court allowed counterclaims by the TPA against the plan sponsor related to negligence and inadequate security of their system but dismissed third-party claims by the custodian against the actual thieves.[3]

Lessons learned

Data compromise alone likely isn't enough to create legal liability for data custodians. When data breaches occur, taking appropriate steps to prevent losses and supporting the use of credit monitoring services go a long way toward mitigating risk.

Plan sponsors must also maintain adequate controls to prevent data breaches for their employees and systems. It isn't enough for plan sponsors to ensure their service providers have adequate cybersecurity programs. If there is a breach anywhere, it can affect the sponsor's plan.

DOL cybersecurity guidance

Now let's consider the DOL's Cybersecurity Program Best Practices.[4] The DOL issued best practices for plan providers along with a list of questions fiduciaries should ask when selecting a service provider. As sub-regulatory recommendations, it's unclear how much weight they'd be given in the context of litigation; however, it's a safe bet that they'll be a consideration when determining who is responsible for cybercrime-related losses.

[1] Ballard, Barclay, "Cybercrime apparently cost the world over $1 trillion in 2020," TechRadar.com, February 15, 2021, https://www.techradar.com/au/news/cybercrime-cost-the-world-over-dollar1-trillion-in-2020.

[2] Kimbriel v. ABB, Inc., No. 5:19-CV-215, 2019 WL 4861168 (E.D.N.C. Oct. 1, 2019), appeal dismissed, No. 19-2243, 2020 WL 2126447 (4th Cir. Jan. 24, 2020): 2019 WL 4861168 at *1.

[3] Leventhal v. M and Marblestone Group, No. 18-cv-2727, 2019 WL 1953247 (E.D. Pa. May 2, 2019). Id. at *7.

[4] U.S. Department of Labor, "Cybersecurity Program Best Practices," accessed June 4, 2021, https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

Some of the foundational best practices put forth by the DOL concern maintaining a robust cybersecurity program including:

- Access controls
- Independent reviews of cyber controls
- Resiliency plans
- Appropriate cyber incident response protocol

Controlling access can prevent the wrong people from breaching your system. Having an independent assessment of your cyber controls can give you additional insight into your program. Resiliency plans and incident response can help prepare for and potentially lessen the impact of fraud when it happens.

What can you do to help defend against cyberthreats – and lawsuits?

Recent litigation and DOL guidance create an informative roadmap to safeguard retirement assets from cybercrime. Consider the following:

1. Having a current and regularly evaluated security program is essential, because the amounts of money are large, cybercriminals are organized, and criminal tactics evolve as security gets better.
2. Fraud can happen at all points of a transaction, and all parties must use prudent security practices to mitigate cyber fraud risk as much as possible.
3. Ensuring that all parties involved with the plan, including third party administrators, trustees, and participants, are educated about cybersecurity threats, such as phishing and social engineering, is paramount. Awareness of these threats and the forms in which they come can help make these threats more easily identifiable and prevent fraud before it happens.
4. Having quick incident response and offering some sort of credit protection for victims of a data breach could prevent losses and thereby prevent litigation.
5. Although compliance with the DOL's best practices isn't required, it may be in your interest to do so.

Using the best practices not only mitigates the risk of ERISA claims or failures, but it also mitigates the risk of negligence claims. Generally, negligence involves failure to act as a reasonable person would. Adhering to the best practices published by the primary regulator of the retirement industry goes a long way toward establishing the reasonableness of your actions.

Not a deposit
Not FDIC-insured
Not insured by any federal government agency
Not guaranteed by any bank or savings association
May go down in value

LincolnFinancial.com

LCN-3615388-060221
PDF 6/21 **Z01**
Order code: DC-LGL02-FLI001

Lincoln Financial Group®

For financial professional and plan sponsor use. Not for use with the public.