Flashpoint: Department of Labor Issues Cybersecurity Guidance (Not to Say We Told You So, But…..)

By: Alison J. Cohen, Esq., APR

Back in 2019, FBLC published our first ***Solution*** regarding the rising threat of identity theft. As we kept hearing of events happening to our clients, and seeing more lawsuits hitting the news, we published a second ***Solution*** in late 2020, regarding the dangers of lax cybersecurity procedures. Earlier this year, we started hearing the first public discussions about cybersecurity and identity theft being on the U.S. Department of Labor's ("DOL") radar. To our great surprise, the DOL quickly produced materials published on April 14, 2021, that can immediately be used by service providers, plan sponsors, and individuals.

Action Plan for Service Providers

If you are a service provider, and you have not already realized that your clients are going to start requesting your cybersecurity policy and procedures, this is your wake-up call. But, here's the good news – the DOL has left you a blueprint to follow. In the "**Cybersecurity Program Best Practices**," the DOL has outlined not only what a service provider should have, such as a formal Cybersecurity Program, but what these documents and best practices should include. According to the DOL, plan service providers should:

- Have a formal, well-documented cybersecurity program
- Conduct prudent annual risk assessments
- Have a reliable annual third-party audit of security controls
- Clearly define and assign information security roles and responsibilities
- Have strong access control procedures
- Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments
- Conduct periodic cybersecurity awareness training
- Implement and manage a secure system development life cycle program
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response
- Encrypt sensitive data, both stored and in transit

- Implement strong technical controls in accordance with best security practices
- Appropriately respond to any past cybersecurity incidents.

This is an overwhelming list if you are new to the cybersecurity arena and you may be wondering where one should even start. Our recommendation is to start with a third-party audit of security controls. Why? Because if there are existing problems with your current system, you are likely too close to the forest to really see the trees … and that concern includes any internal IT folks you may have. You want to bring in an outside IT firm that really specializes in this sort of review and boldly face the monsters that may be living under your bed. Once you have a sense of the strengths (or weaknesses) of your current system, you can then build on it.

Creating or modifying your formal cybersecurity program based on what you learn from your IT audit experience would be the next logical step. The IT firm may even be able to help you create the program. The program now becomes the basis for employee training and setting the roles and responsibilities within your business for maintaining the program. Think of it as the foundation for all of the other pieces that need to snap into place. Not only does all of this protect your clients and their participants, but it also protects you from potential breaches and resulting financial losses.

One last piece to which you need to give a lot of thought is a business continuity program. Everyone experienced some degree of business continuity issues in the past year. The pandemic required many businesses to learn how to pivot suddenly so that their people could work outside of the office space. But what if things go past just the inability to reach the office? What if there is a true catastrophe? A 9.0 earthquake? Another Hurricane Katrina, tornado, a flood, or massive fire? Your office may be entirely destroyed. What then? In California, on the third Thursday in October each year, there is the ShakeOut Day. It's an opportunity for business owners to conceptualize and practice what they may need to do in the event of a true disaster. This exercise is tremendously useful and shouldn't be restricted to just California. Every year, you can identify potential weaknesses and shore them up gradually, so it's not overwhelming.

Tips Given for Plan Sponsors

The DOL also produced "**Tips for Hiring a Service Provider with Strong Cybersecurity Practices.**" If you are a service provider and your practice already complies with these "tips," you should market this as one of your company's strengths. You can point out to potential clients why your firm may be better than others because you have mastered the above action plan.

If you are a plan sponsor, you should be asking both existing and prospective service providers about their security protocols, third-party audits, security reporting, and procedures in the event of a breach. If the service provider's service agreement doesn't have any language addressing these important practices, this is a red alert for you as the plan sponsor. As this issue becomes more and more mainstream, service providers will find themselves losing business due to this delinquency.

As a plan sponsor, you are responsible for hiring service providers who will protect your participants' assets. You could be liable for damages if you hire a service provider that is missing these important practices and protocols, particularly if their service agreement was silent and you didn't raise the issue. Recently, Abbott Labs was dismissed as a defendant in a lawsuit filed in relation to an identity theft claim. In part, the Court found there was no evidence that Abbott Labs was negligent in hiring its service provider, Alight. Now, imagine how different this decision could have been had there been evidence that the service provider and its contract did not address

cybersecurity, and if during the hiring process, Alight admitted it had no protocols in place. It is very possible that the Court would have reached a different conclusion.

Best Practices for Individuals

Much of the identity theft and cyberthreats start with us as individuals and the choices that we make. The DOL didn't forget about this either. Many of the security tips given by the DOL are items that were highlighted in our earlier Solutions articles. If you haven't taken steps yet, you need to adopt these habits:

- Register, set up, and routinely monitor your online accounts
- Use strong and unique passwords
- Use multi-factor authentication whenever offered
- Keep your personal contact information (address, email, phone number) current on accounts
- Close or delete unused accounts
- Beware of phishing attacks
- STAY AWAY from free wi-fi (think of this like a gas station restroom)
- Use antivirus software and keep apps/software current.

When bad things happen, the DOL has also given us reporting tools to use. I know that many of us don't believe that the justice system really works, but we have seen proof of prosecutions that have occurred because of diligent reporting done by victims. If you or a loved one has been a victim of identity theft or cybersecurity breaches, you can report these to:

https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view

https://www.cisa.gov/reporting-cyber-incidents

Concluding Thoughts

None of us can avoid dealing with the impact of identity thieves and cyber-pirates. And, as much as we have other things that we'd prefer to be doing, turning a blind eye can result in a participant's loss of hard-earned retirement funds and one of the worst days of a service provider's professional life. Now that the DOL has started to issue guidance, it is reasonable to expect that federal regulations will come down the road eventually and that this guidance will be part of the substance of DOL investigations in the future. It's better that we work with the tips given and develop strong practices now to get ahead of the curve.

If you are a service provider and need help with your service agreement, or if you are a provider or a plan sponsor that needs help with an unfortunate breach incident, give us a call. After all, ***we are your ERISA solution***!

FERENCZY
BENEFITS LAW CENTER
We are your ERISA solution™

Ilene Ferenczy • ilene@ferenczylaw.com | Alison Cohen • acohen@ferenczylaw.com
Adrienne Moore • amoore@ferenczylaw.com | Adriana Starr • astarr@ferenczylaw.com
Tia Thornton • tthornton@ferenczylaw.com | Leah Dean • ldean@ferenczylaw.com

2635 Century Parkway Suite 200, Atlanta, GA 30345
T 404.320.1100 | F 404.320.1105 | www.ferenczylaw.com