PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

REPORT ON

VENDOR DUE DILIGENCE ASSESSMENT

PRESENTED TO

Trustees of the

Warehouse Employees Union Local No. 730 & Contributing Companies' Prepaid Legal Services Funds

November 20, 2023

Submitted by:
Thomas J. DeMayo, CISSP, CISA, CRISC, CIPP/US, MCSE, CEH, CCFE, CHFI, CPT
Partner, Cybersecurity and Privacy Advisory
Cyber Risk Management Group
tdemayo@pkfod.com

KNOW GREATER VALUE®

November 20, 2023

To the Trustees of the Warehouse Employees Union Local No. 730 & Contributing Companies' Prepaid Legal Services Funds

Dear Trustees:

PKF O'Connor Davies Advisory, LLC has completed the performance of Vendor Due Diligence on behalf of the Warehouse Employees Union Local No. 730 & Contributing Companies' Prepaid Legal Services Funds ("the Funds"). The objective of the study was to review the alignment of the utilized Vendors' cybersecurity programs with the cybersecurity guidance issued by the Department of Labor.

Any procedures that were performed by us in connection with this assignment did not constitute an audit and were not designed to provide, and we will not express, any assurance on internal control.

Our findings are summarized within this report.

This report is intended solely for the information and use of the Funds.

We wish to thank you and your staff for the courtesy and cooperation extended to us.

Very truly yours,

PKF O'Connor Davies Advisory, LLC

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS
ESTABLISHED IN 1891

Table of Contents

Vendor Due Diligence Assessment

RISK RANKING DEFINITION

Based on the responses provided, the below rating system was applied to the Vendors in relation to their Cybersecurity Maturity level.

1. **No Response or Response Refused** – The Vendor has not provided any information for the assessment, stopped responding for follow-up information, or never responded to the initial requests.

2. **Low Maturity** – The Vendor has not implemented many of the minimum-security controls specified by the Department of Labor.

3. **Moderate Maturity –** The Vendor meets the majority of the security controls specified by the Department of Labor.

4. **Moderate-High Maturity** – The Vendor meets almost all of the security controls specified by the Department of Labor with minor deviations.

5. **High Maturity** – The Vendor meets all the security requirements specified by the Department of Labor.

For one of the Vendors, Sinder Law we assigned either a Satisfactory or Non-Satisfactory ranking. The reason for the deviation is that the Vendor is very small in size and limited in resources. Full alignment with the DOL Guidance would be unrealistic and unreasonable.

1. **Satisfactory** – Reasonable security controls have been implemented to mitigate the material risks to the information stored, processed, and/or transmitted.

2. **Non–Satisfactory** – Basic and key security controls were missing relative to the risks of the information stored, processed, and/or transmitted.

CYBERSECURITY ASSESSMENT RISK BREAKDOWN

During this assessment, we reviewed specific security controls for each vendor in accordance with the controls specified by the Department of Labor. The individual control areas assessed were:

- **A Well Documented Cybersecurity Program** – The Vendor should have a formalized and well-documented Information Security Program.

- **Annual Risk Assessments** – The Vendor performs an annual risk assessment to assist in determining any security gaps within the multiple areas within their Organization.

- **Reliable Third-Party Audit of Controls** – The Vendor performs Vulnerability scanning,

Penetration Testing, or any other type of Security Testing by a reliable Outsourced company.

- **Clearly Defined Information Security Roles and Responsibilities** – The Vendor has specified employees which are placed in charge of handling Cybersecurity for their Organization and those employees understand their job responsibilities.

- **Strong Access Control Procedures**– The Vendor has implemented Two Factor authentication for any remote access into their environment and has implemented the principle of least privilege.
- **Vendor Due Diligence**– The Vendor is utilizing a third-party cloud service provider and is performing their vendor due diligence by annually reviewing their security controls by asking for an SOC 2 type II report or sending out a questionnaire verifying they are following security best practices.

- **Annual Cybersecurity Awareness Training** – The Vendor is enforcing annual Cybersecurity Awareness training for all employees. The training includes anything new on the annual Risk Assessment report and a periodic Phishing test.

- **A Software Development Lifecycle** – The Vendor has a Software Development Lifecycle for their custom developed Software, or they do not have one because they do not custom develop software. In which case, this requirement cannot be applicable.

- **Disaster Recovery and Business Continuity Plans** – The Vendor has formalized Disaster Recovery and Business Continuity Plans in the event of a disaster event.

- **Encryption of Sensitive Data at Rest and in Transit** – The Vendor is properly encrypting all sensitive data stored on systems and being sent over a network connection**.**

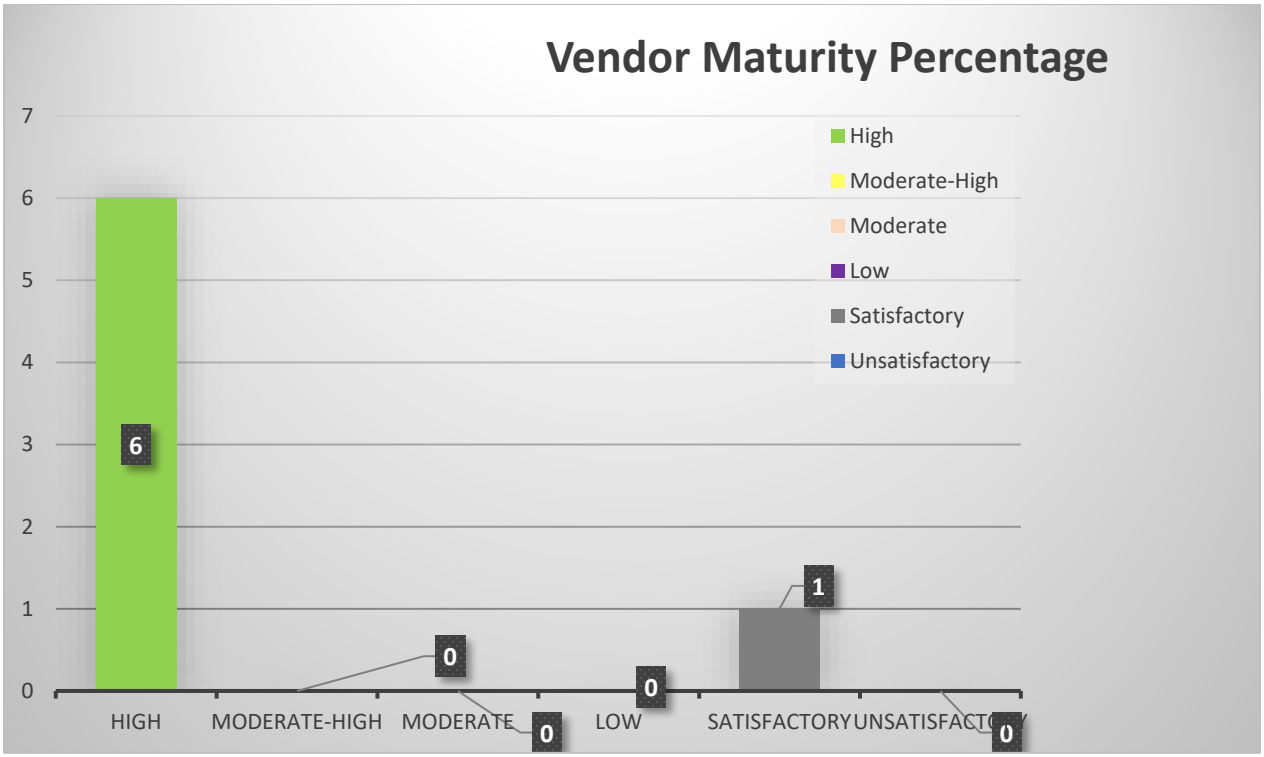
- **Security Best Practices and Technical Controls** – The Vendor is implementing security configuration best practices (Password controls, proper access controls, etc.) and proper security appliances (firewalls with IDS/PS, web content filter, Antivirus/EDR, etc.).

EXECUTIVE SUMMARY

In total, we reviewed **7** Vendors. Each vendor was given a qualitative risk ranking of High, Moderate-High, Moderate, Low or Non-Responsive. Of the **7** vendors, the number of risks for each risk ranking is as follows:

Maturity Level	Total
High	6
Moderate-High	0
Moderate	0
Low	0
Satisfactory	1
Unsatisfactory	0

The chart below represents the total maturity percentage of the vendors assessed.



Based on the chart above, the majority of the Organization's vendors are at a High level of Cybersecurity Maturity.

SINDER LAW CONSIDERATION

Sinder Law, as noted prior, is a small entity consisting of one attorney. Sinder Law does have an IT Support person that facilitates the handling of key security controls such as vendor security patch installation and malware monitoring. Historically, Sinder Law received a large amount of member sensitive data, this data was saved on the office computers local hard drive. At the time of our detailed conversation with Sinder Law, the process had changed such that no sensitive information is sent to Sinder Law as it is not needed for the services provided. While the process had changed, the historical data remained. To remediate the issue, we recommend that the Fund request that Sinder Law delete all historical files that contain sensitive information.

ONGOING APPROACH

The initial year review as designed was sufficient to establish a baseline of maturity and risk across the Vendors in relation to the DOL Cybersecurity Guidance. The limitations of strictly going by the DOL Guidance, as we have learned, is that it has a tendency to be broad and the vendor responses reflected that. We believe this methodology is only effective for year one to establish the general baseline and also make the Vendors accustomed to the process and expectations. For many of the Vendors, it took a lot of back and forth to make them understand a generic and limited answer was not going to be sufficient for us and the expectations were higher than they perceived. We recognize the Funds may not want to do this every year, as such, the following proposed approach for subsequent years is as follows:

- Each Vendor is formally risk assessed to determine the risk of the Vendor to the Funds. The risk assessment should factor in the overall results of this assessment, their size, and maturity. Any Vendor identified as having Low or Moderate maturity based on this assessment will automatically be considered a High risk vendor and be reassessed in the subsequent year to identify remediation progress. Vendors with Low or Moderate maturity will be reassessed annually until their ranking changes to Moderate-High or High.

- Any Vendor identified as a Moderate-High or High maturity must be reassessed at a frequency of every-other year or once every three years.

- Any Vendor that experiences a breach that materially impacts the Funds, and their members will be deemed a High risk vendor for a period of three years and will be re-assessed annually during that period.

- A detailed questionnaire should be created that lists very specific controls that should be implemented. Controls will be weighted based on criticality. Such a method will allow us to generate a quantitative scoring process for the Vendors. In addition, it will help advise Vendors of controls that we believe are critical and need to be implemented if not. We will provide a suggested form to use going forward for any new Vendor and subsequent assessments.

The above is a risk-based approach to the Vendors. Should the Funds desire a full review every year or have a different proposed method, we will accommodate accordingly, should we continue to assist the Funds.

VENDOR MATURITY SUMMARY

Vendor	Maturity Level	Security Controls – Not Implemented/No Response, Hardly, Mostly, Partially, or Fully Implemented	Number of Cybersecurity Practice Deficiencies Discovered
Associated Administrators, LLC	**High**	**Fully Implemented**	**0**
Investment Performance Services	**High**	**Fully Implemented**	**0**
Morgan Lewis	**High**	**Fully Implemented**	**0**
Novak Francella	**High**	**Fully Implemented**	**0**
NFP	**High**	**Fully Implemented**	**0**
PNC Bank	**High**	**Fully Implemented**	**0**
Sinder Law	**Satisfactory**		