Warehouse Employees Union Local No. 730 and Contributing Companies' Prepaid Legal Services Fund

911 Ridgebrook Road
Sparks, Maryland 21152-9451
Telephone: (800) 730-2241
www.associated-admin.com

8400 Corporate Drive, Suite 430
Landover, Maryland 20785-2361
Telephone: (800) 730-2241
www.associated-admin.com

Agenda

September 1, 2021
9:00 AM

I. Call to Order

II. Minutes, Regular Meeting – June 10, 2021

III. Financial Report – Investment Performance Services

IV. Auditor Report

V. Counsel Report

VI. Administrative Manager Report

VII. Invoices

VIII. Other Fund Business

IX. Next Meeting Date and Location

X. Adjournment

Warehouse Employees Union Local No. 730
and Contributing Companies' Prepaid
Legal Services Fund

911 Ridgebrook Road
Sparks, Maryland 21152-9451
Telephone: (800) 730-2241
www.associated-admin.com

8400 Corporate Drive, Suite 430
Landover, Maryland 20785-6102
Telephone: (800) 730-2241
www.associated-admin.com

DRAFT

MINUTES OF THE MEETING OF THE BOARD OF TRUSTEES OF THE WAREHOUSE EMPLOYEES UNION LOCAL NO. 730 & CONTRIBUTING COMPANIES' PREPAID LEGAL SERVICES FUND JUNE 10, 2021 VIA TELECONFERENCE

The following Trustees were present:

UNION TRUSTEES
R. Brooks – Chairman
L. Hudson
J. Venable

EMPLOYER TRUSTEES
M. Bull – Secretary
J. Paradis
H. Sebhat
M. Goble – Alternate

Also present were:

A. Cochran – Associated Administrators, LLC
M. DeLancey – Blank Rome LLP
R. Grant – Associated Administrators, LLC
R. Sichel – Investment Performance Services, LLC

I. CALL TO ORDER

A quorum being present, the meeting was called to order.

II. MINUTES

The Trustees reviewed the minutes of the last regular meeting held March 26, 2021.

Trustee Bull requested additional details for the Blank Rome LLP fee request including the percentage increase and effective date of the last rate increase.

On MOTION made and seconded, the Trustees voted unanimous approval of the following resolution:

> **RESOLVED that the minutes of the last regular meeting held on March 26, 2021 approved as revised to include the above noted changes.**

III. FINANCIAL REPORT

A. Custodian Bank – PNC Bank, NA

Ms. Cochran noted a copy of the PNC Summary of Activity report for the period January 1, 2021 through March 31, 2021 is contained in the meeting booklet.

B. Investment Performance Services, LLC ("IPS")

The Trustees welcomed Mr. Rich Sichel of IPS to the meeting.

Mr. Sichel reviewed his report titled, "Investment Performance Analysis – March 31, 2021" beginning with IPS' market commentary. Mr. Sichel noted the asset allocation as follows: 58.40% in Investment Grade Income, 35.50% in Short Duration High Yield Fixed Income, and 6.20% in cash and equivalents. The Atlanta Capital Bond Fund held $550,897 in investments, and the Chartwell Short Duration High Yield Fund held $334,629. The PNC Prime Money Market held $58,095.

Mr. Sichel noted that the Investment Grade Fixed Income allocation is not within the targeted policy range of the Investment Policy Statement. Mr. Sichel recommended that the Trustees rebalance the Fund's Investment Grade Fixed

Income allocation by re-allocating $18,000 to Short Duration High Yield Fixed Income.

On MOTION made and seconded, the Trustees voted unanimous approval of the following resolution:

RESOLVED to follow IPS' recommendation to rebalance assets by allocating $18,000 from Investment Grade Fixed Income to Short Duration High Yield Fixed Income.

The Trustees thanked Mr. Sichel for his report, and he was excused from the meeting.

IV. COUNSEL REPORT

Mr. DeLancey said there were no legal matters pending before the Board of Trustees at this time.

V. ADMINISTRATIVE MANAGER'S REPORT

Ms. Cochran presented the Administrative Manager's Report for the first quarter 2021. Such report showed employer contributions of $21,967, miscellaneous income of $0 and interest and dividend income of $5,712, producing a total income of $27,679 for the quarter. Benefit expenses were $4,840 and operating expenses were $6,767, producing a total expense of $11,607, resulting in a net surplus of $16,072 for the quarter. Ms. Cochran noted that contributions were made on behalf of 641 participants.

VI. INVOICES

Ms. Cochran presented a list of invoices dated June 10, 2021 for Trustee review. It was noted that there were no additions, deletions or changes to the list.

On MOTION made and seconded, the Trustees voted unanimous approval of the following resolution:

RESOLVED that the invoices on the list dated June 10, 2021 are approved for payment as presented.

VII. OTHER FUND BUSINESS

A. Fiduciary Liability Insurance Renewal and Waiver of Recourse Premiums

Ms. Cochran stated the Fiduciary Liability Policy expires July 26, 2021. She requested proposals from NFP and Segal, per Trustee direction. Ms. Cochran reported that the renewal proposals are not yet available but will be distributed for review prior to the next meeting.

B. 2020 Summary Annual Report

Ms. Cochran reported that Novak Francella performed fieldwork for the audit in the Administrative Manager's office the week of May 24, 2021. Due to the timing of the fieldwork, draft financials are not yet available. She said the auditor expected to file the Form 990 and Form 5500 on time, however would like to request approval to file for extensions in case of an unforeseen delay.

On MOTION made and seconded, the Trustees voted unanimous approval of the following resolution:

RESOLVED to approve Novak Francella to file an extension for the Form 990 and Form 5500.

VIII. NEXT MEETING DATE AND LOCATION

After discussion, the Trustees selected September 1, 2021 as their next regular meeting in Landover, Maryland.

IX. ADJOURNMENT

There being no additional business to come before the Trustees, the meeting was adjourned.

Respectfully submitted,

Michael Bull
Secretary

WAREHOUSE LOCAL 730 - PREPAID LEGAL FUND
SUMMARY OF ACTIVITY
JANUARY 01, 2021 to JUNE 30, 2021

	Cash Reserve	Atlanta Capital	Total
Beginning Market Value	$379,083	$551,724	$930,807
Receipts	$45,759	$0	$45,759
Disbursements	$40,246	$0	$40,246
Inter-Account Transfers	$138,000	$138,000	$0
Earnings	$7,117	$66	$7,049
Ending Market Value	**$529,713**	**$413,658**	**$943,371**

PNC BANK, NA

Warehouse Employees Union Local No. 730 and Contributing Companies' Prepaid Legal Services Fund

Cybersecurity Policy

I. Statement of Purpose

The purpose of this Cybersecurity Policy ("Policy) is to assist the Board of Trustees ("Trustees") of the Warehouse Employees Union Local No. 730 and Contributing Companies' Prepaid Legal Services Fund("Fund") in prudently monitoring the cybersecurity practices of those that interact electronically, or will interact electronically, with the Fund in accordance with the fiduciary requirements of the Employee Retirement Income Security Act of 1974, as amended ("ERISA").

This Policy does not impose any duties on the Trustees beyond those already imposed by ERISA. Recognizing the tension between the most secure cybersecurity practices and the user experience for the Fund's participants, this Policy does not require the Fund's Third-Party Administrator (TPA) or the TPA's Information Technology ("IT") professionals and/or the Fund's other service providers to adopt the most stringent version of every security practice identified in the guidance addressing the cybersecurity practices of those interacting with ERISA-covered employee benefit plans (the "Cybersecurity Guidance") issued by the Department of Labor ("DOL") in April, 2021. Rather, this Policy defers to the Trustees, in conjunction with technical experts, as appropriate, to determine what practices are prudent for mitigating the Fund's exposure to cybersecurity events.

II. Policy Goals & Objectives

This Policy is designed to serve as a guide for the Trustees with respect to the cybersecurity practices of the Fund's service providers with significant electronic access to the Fund's information and/or control over Fund's assets (each a "Service Provider" and collectively the "Service Providers"), the Fund's TPA, and its IT professionals, and the Fund's participants. As such, the Policy is not intended to serve as a rigid framework for the Trustees. The Trustees may deviate from this Policy in their discretion where they deem appropriate to do so in the best interest of the Fund's participants.

In general, the Policy is designed to:

- Outline the roles and responsibilities of the Trustees, Service Providers, TPA, and Fund participants in mitigating cybersecurity risk;
- Outline a prudent process for the Trustees to evaluate cybersecurity risk in engaging or re-engaging Service Providers; and
- Outline guidelines for the Trustees to use in monitoring existing Service Providers with respect to cybersecurity risk.

III. Roles & Responsibilities

Mitigating cybersecurity risk implicates a number of parties, including: the Trustees, the TPA and its IT Professionals, Service Providers, and Fund participants. The following summarizes the roles and responsibilities of these parties.

The Trustees

The Trustees will seek to mitigate risk of loss to and fraud on the Fund through the prudent selection and monitoring of Service Providers.

In accordance with this Policy, the Trustees will review the cybersecurity practices of Service Providers when engaging (or re-engaging) the Service Providers and periodically while the Service Providers are providing services to the Funds. The Trustees may, as they deem necessary or appropriate, enlist IT professionals to assist in the evaluation of Service Providers' cybersecurity practices. The Trustees (with the assistance of counsel) will endeavor to obtain contractual protections consistent with then-current industry standards from the Service Providers with respect to cybersecurity matters.

The Trustees will work to educate Fund participants on strong cybersecurity practices and their responsibility to help mitigate the Fund's exposure to cybersecurity events.

TPA and TPA's IT Professionals

The TPA and the TPA's IT professionals will continue to evaluate and improve the Fund's cybersecurity practices to minimize the risk of cybersecurity threats to the TPA's IT system, which stores confidential Fund and Fund participant information.

Service Providers

Service Providers play an integral role in the operation of the Fund and may have significant access and/or control over the Fund's information and assets. The Trustees will seek confirmation from the Fund's Service Providers that such entities have and maintain appropriate cybersecurity practices to mitigate the Fund's and its participants' exposure to cybersecurity events.

Fund Participants

The Fund's participants play an important role in protecting the Fund from cybersecurity events and fraudulent distributions. The Trustees will seek to encourage participants to follow safe cybersecurity practices and protect the confidentiality of their Fund account password and related identifying information, and notifying the Trustees and/or the Service Providers in the event of a cybersecurity event.

IV. Engaging or Re-engaging Service Providers

When engaging (or re-engaging) a Service Provider, the Trustees will inquire as to the cybersecurity practices adopted by the Service Provider and shall consider these practices when deciding whether to engage (or re-engage) the Service Provider. While the Trustees shall recognize the importance of strong cybersecurity practices, the evaluation of the Service Provider's cybersecurity practices will be only one factor of the Trustees' more fulsome evaluation of whether it would be prudent to engage (or re-engage) the Service Provider.

When evaluating the Service Provider's cybersecurity practices, the Trustees shall consider the DOL's *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* (attached as Appendix A). The Trustees, in consultation with counsel, may consider the following when deciding whether to engage the Service Provider:

1. The Service Provider's security standards, practices and policies, and audit results, as compared to industry standards.
2. The process that the Service Provider uses to validate its cybersecurity practices, and the levels of security standards that it has met and implemented.
3. The Service Provider's track record in the industry, including any public information addressing security events, litigation, or legal proceedings regarding the Service Provider's services.
4. Whether the Service Provider has experienced any security breaches in the past, the context of the breaches, and how the Service Provider addressed the situation.
5. Whether the Service Provider possesses any cybersecurity or identity theft insurance.
6. Applicable contractual provisions for the Service Provider's ongoing cybersecurity and information security compliance, including provisions addressing (A) information security reporting, (B) confidentiality and the permitted use of Plan information, (C) notice in the event of a cybersecurity breach, (D) compliance with record retention, privacy, and information security laws, and (E) the adequacy of the Service Provider's cybersecurity and errors and omissions insurance.

In deciding whether to engage or re-engage a Service Provider, the Trustees may also consider other factors, including those outlined below pertaining "cybersecurity program best practices."

V. Monitoring Existing Service Providers

The Trustees will establish a process for monitoring the cybersecurity practices of Service Providers on an ongoing basis to ensure they adequately protect the Fund and its participants against cybersecurity threats. While the Trustees shall recognize the importance of strong cybersecurity practices, the evaluation of the Service Provider's cybersecurity practices will be only one factor of the Trustees' more fulsome process for deciding whether it is prudent to continue to retain the Service Provider.

In establishing a process for monitoring the Service Provider's cybersecurity practices, the Trustees shall consider the DOL's *Cybersecurity Program Best Practices* (attached as Appendix B). The Trustees' process for deciding whether it is prudent to retain the Service Provider may consider whether the Service Provider:

1. has a formal, well documented cybersecurity program.
2. conducts prudent annual risk assessments.
3. receives a reliable third-party audit of security controls on a yearly basis.
4. clearly defines and assigns information security roles and responsibilities among its employees.
5. has strong access control procedures (including multi-factor authentication).
6. has a process in place for ensuring that Plan data and assets held in a cloud or managed by a third-party service provider are maintained with adequate security reviews and independent security evaluations.
7. conducts regular, updated cybersecurity trainings for personnel.
8. implements and maintains a secure System Development Life Cycle Program (SDLC).
9. implements and maintains an effective Business Continuity and Disaster Recovery (BCDR) Program, which also addresses incident response.
10. encrypts Plan and other sensitive information (stored and in transit).
11. implements robust technical controls in accordance with current best security practices.
12. has timely and appropriately responded to any past cybersecurity events.

VI. Informing Participants of their Cybersecurity Obligations

The Trustees will communicate with the Funds' participants regarding their obligations to mitigate their own and the Funds' exposure to cybersecurity events. In communicating with the Funds' participants regarding their cybersecurity responsibilities and the best ways to protect their accounts, the Trustees shall consider the DOL's *Online Security Tips* (attached as Appendix C).

* * * * *

It is understood that this Cybersecurity Policy Statement is meant to provide a general framework to assist the Trustees with fulfilling their fiduciary duties under ERISA. The practices described herein serve as one, reasonable approach to mitigating the Fund's exposure to cybersecurity threats. Changing market conditions, economic trends or business needs may necessitate that the Trustees modify this Policy or disregard this Policy in whole or in part. This Policy may be modified by written approval of the Trustees.

To: [Name of Service Provider]

Subject: DOL Cybersecurity Guidance

Dear_____,

The Department of Labor ("DOL") recently issued new cybersecurity guidance that impacts ERISA plans. The DOL has started enforcement actions focusing on plan and service provider cybersecurity practices and the best practices cited in the DOL guidance, which is attached, are the new required standards. Our attorneys have reviewed cybersecurity-specific audit requests issued by the DOL and confirmed that these requests specifically inquire about service providers' cybersecurity practices and the steps that a plan's trustees have taken to monitor the service provider's cybersecurity practices.

In light of this new DOL guidance and enforcement initiative, we ask that you please document the steps [SERVICE PROVIDER] has or is taking to assist the plan and its trustees to ensure compliance with the new DOL guidance? We would appreciate your review and responses to the questions below by DATE, 2021. [2-3 week timeframe]

1. Please describe your current data security standards, practices, and policies? Do you follow a recognized standard for information security?

2. Does [SERVICE PROVIDER] have a formal cybersecurity program? If so, please provide a copy or information about the program? Additionally, please confirm that the formal cybersecurity program addresses:
    a. data privacy, governance, and custody (including encryption and other practices relating to the storage of plan information on laptops and mobile devices); and
    b. the use of access controls, firewalls, multi-factor authentication, unique complex passwords, the regular updating of such passwords, and other methods of protecting plan assets and data.

    If these issues are not addressed in [SERVICE PROVIDER'S] formal cybersecurity program, please summarize [SERVICE PROVIDER'S] approach to these issues.

3. Please indicate if you have an annual cybersecurity audit or risk assessment. If so, please summarize the techniques used as part of the assessment (e.g., penetration tests, third-party cybersecurity analyses, etc.) and whether the assessment includes information regarding [SERVICE PROVIDER'S] compliance with its established internal controls. Please share the results of any such assessment as well as how the results compare against industry standards.

4. Does [SERVICE PROVIDER] use a third-party auditor to assess security controls on an annual basis? If so, are annual findings available to plan sponsors? Do these annual audit reports verify information security, system/data availability, processing integrity, and data confidentiality?

5. If available, please provide us with your most current Service Organization Control audit reports (SOC 1, SOC 2, and/or SOC 3). If you are not able to provide any such report, please describe the process that is used to audit your recordkeeping system and provide an auditor's report addressing your recordkeeping system.

6. Please provide a policy or description of the control procedures in place to limit access to plan and participant data to only authorized users?

7. Please provide a description of security review and/or procedures for assessment of cloud-based or third-party managed storage systems used by [SERVICE PROVIDER] or third parties hired by [SERVICE PROVIDER] to service the plan?

8. Please provide a description of [SERVICE PROVIDER'S] business resiliency program to maintain business continuity in the event of an incident or disaster? When was the last time the business resiliency program was reviewed to ensure consistency with industry best practices?

9. Have you developed and implemented a system development life cycle (SDLC) to manage systems and a vulnerability management plan? When was the last time the SDLC and vulnerability management plan was reviewed to ensure consistency with industry best practices? Are regular penetration tests conducted on customer-facing applications?

10. Please provide a description of the education and training provided to personnel that service the plan to ensure that they are aware of [SERVICE PROVIDER'S] cybersecurity practices and potential cybersecurity threats?

11. Please describe any past security events and summarize your responses to those events? Were plan assets or plan data affected by any of these security events?

12. Please confirm that your insurance coverage covers losses relating to cybersecurity and identity theft events, the amount of such coverage, and that such coverage is current?

13. Please confirm whether our service agreement with [SERVICE PROVIDER] includes existing provisions responsive to this new guidance? If revisions to our agreement will be proposed to ensure continued compliance with these standards, when would these revisions be effective?

14. Do you use contractors or subcontractors to service the plan? If so, does [SERVICE PROVIDER] monitor their cybersecurity practices? And are they contractually obligated to have cybersecurity practices that are at least as stringent as [SERVICE PROVIDER'S] cybersecurity practices?

15. Do you use plan data for any purposes other than servicing the plan? If so, please describe the purposes for which you use plan data and the steps that you take to protect this data after it is extracted from the plan.

Thank you in advance for your help in ensuring our plan is compliant with the newly issued guidance.

Regards,

TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

As sponsors of 401(k) and other types of pension plans, business owners often rely on other service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices.

To help business owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor such service providers, we prepared the following tips for plan sponsors of all sizes:

1. Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions.
    - Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity. You can have much more confidence in the service provider if the security of its systems and practices are backed by annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality.

2. Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.

3. Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.

4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.

5. Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participants' account).

6. When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware contract provisions that limit the service provider's responsibility for IT security breaches. Also, try to include terms in the contract that would enhance cybersecurity protection for the Plan and its participants, such as:
    - **Information Security Reporting**. The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.

- **Clear Provisions on the Use and Sharing of Information and Confidentiality**. The contract should spell out the service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse.
- **Notification of Cybersecurity Breaches**. The contract should identify how quickly you would be notified of any cyber incident or data breach. In addition, the contract should ensure the service provider's cooperation to investigate and reasonably address the cause of the breach.
- **Compliance with Records Retention and Destruction, Privacy and Information Security Laws**. The contract should specify the service provider's obligations to meet all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information.
- **Insurance**. You may want to require insurance coverage such as professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and/or fidelity bond/blanket crime coverage. Be sure to understand the terms and limits of any coverage before relying upon it as protection from loss.

CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. 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.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

1. A Formal, Well Documented Cybersecurity Program.

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudently designed program will:

Protect the infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- **Identify** the risks to assets, information and systems.
- **Protect each of the necessary assets, data and systems.**
- **Detect and respond to** cybersecurity events.
- **Recover** from the event.
- **Disclose the event as appropriate**.
- **Restore normal operations and services**.

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approval by senior leadership.
- Review at least annually with updates as needed.
- Terms are effectively explained to users.
- Review by an independent third party auditor who confirms compliance.
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

- Formal and effective policies and procedures governing all the following:
  1. Data governance and classification.
  2. Access controls and identity management.
  3. Business continuity and disaster recovery.
  4. Configuration management.
  5. Asset management.
  6. Risk assessment.
  7. Data disposal.
  8. Incident response.
  9. Systems operations.
  10. Vulnerability and patch management.
  11. System, application and network security and monitoring.
  12. Systems and application development and performance.
  13. Physical security and environmental controls.
  14. Data privacy.
  15. Vendor and third party service provider management.
  16. Consistent use of multi-factor authentication.
  17. Cybersecurity awareness training, which is given to all personnel annually.
  18. Encryption to protect all sensitive information transmitted and at rest.

2. Prudent Annual Risk Assessments.

A Risk Assessment is an effort to identify, estimate, and prioritize information system risks. IT threats are constantly changing, so it is important to design a manageable, effective risk assessment schedule. Organizations should codify the risk assessment's scope, methodology, and frequency. A risk assessment should:

- Identify, assess, and document how identified cybersecurity risks or threats are evaluated and categorized.
- Establish criteria to evaluate the confidentiality, integrity, and availability of the information systems and nonpublic information, and document how existing controls address the identified risks.
- Describe how the cybersecurity program will mitigate or accept the risks identified.
- Facilitate the revision of controls resulting from changes in technology and emerging threats.
- Be kept current to account for changes to information systems, nonpublic information, or business operations.

3. A Reliable Annual Third Party Audit of Security Controls.

Having an independent auditor assess an organization's security controls provides a clear, unbiased report of existing risks, vulnerabilities, and weaknesses.

As part of its review of an effective audit program, EBSA would expect to see:

- Audit reports, audit files, penetration test reports and supporting documents, and any other analyses or review of the party's cybersecurity practices by a third party.
- Audits and audit reports prepared and conducted in accordance with appropriate standards.
- Documented corrections of any weaknesses identified in the independent third party analyses.

4. Clearly Defined and Assigned Information Security Roles and Responsibilities.

For a cybersecurity program to be effective, it must be managed at the senior executive level and executed by qualified personnel. As a senior executive, the Chief Information Security Officer (CISO) would generally establish and maintain the vision, strategy, and operation of the cybersecurity program which is performed by qualified personnel who should meet the following criteria:

- Sufficient experience and necessary certifications.
- Initial and periodic background checks.
- Regular updates and training to address current cybersecurity risks.
- Current knowledge of changing cybersecurity threats and countermeasures.

5. Strong Access Control Procedures.

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to IT systems and data. It mainly consists of two components: authentication and authorization. The following are best security practices for access control:

- Access to systems, assets and associated facilities is limited to authorized users, processes, devices, activities, and transactions.
- Access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) are limited based on the role of the individual and adhere to the need-to-access principle.
- Access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with policy.
- All employees use unique, complex passwords.
- Multi-factor authentication is used wherever possible, especially to access the internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control methodology.
- Policies, procedures, and controls are implemented to monitor the activity of authorized users and detect unauthorized access, use of, or tampering with, nonpublic information.
- Procedures are implemented to ensure that any sensitive information about a participant or beneficiary in the service provider's records matches the information that the plan maintains about the participant.
- Confirm the identity of the authorized recipient of the funds.

6. 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.

Cloud computing presents many unique security issues and challenges. In the cloud, data is stored with a third-party provider and accessed over the internet. This means visibility and control over that data is limited. Organizations must understand the security posture of the cloud service provider in order to make sound decisions on using the service.

Best practices include:

- Requiring a risk assessment of third party service providers.
- Defining minimum cybersecurity practices for third party service providers.
- Periodically assessing third party service providers based on potential risks.

- Ensuring that guidelines and contractual protections at minimum address the following:
  - » The third party service provider's access control policies and procedures including the use of multi-factor authentication.
  - » The third party service provider's encryption policies and procedures.
  - » The third party service provider's notification protocol for a cybersecurity event which directly impacts a customer's information system(s) or nonpublic information.

7. Cybersecurity Awareness Training Conducted at Least Annually for All Personnel and Updated to Reflect Risks Identified by the Most Recent Risk Assessment.

Employees are often an organization's weakest link for cybersecurity. A comprehensive cybersecurity security awareness program sets clear cybersecurity expectations for all employees and educates everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat. Since identity theft is a leading cause of fraudulent distributions, it should be considered a key topic of training, which should focus on current trends to exploit unauthorized access to systems. Be on the lookout for individuals falsely posing as authorized plan officials, fiduciaries, participants or beneficiaries.

8. Secure System Development Life Cycle Program (SDLC).

A secure SDLC process ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort. Best practices include:

- Procedures, guidelines, and standards which ensure any in-house applications are developed securely. This would include such protections as:
  - » Configuring system alerts to trigger when an individual's account information has been changed.
  - » Requiring additional validation if personal information has been changed prior to request for a distribution from the plan account.
  - » Requiring additional validation for distributions (other than a rollover) of the entire balance of the participant's account.
- Procedures for evaluating or testing the security of externally developed applications including periodic reviews and updates.
- A vulnerability management plan, including regular vulnerability scans.
- Annual penetration tests, particularly with respect to customer-facing applications.

9. A Business Resiliency Program which Effectively Addresses Business Continuity, Disaster Recover, and Incident Response.

Business resilience is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data. The core components of a program include the Business Continuity Plan, Disaster Recovery Plan, and Incident Response Plan.

- The Business Continuity Plan is the written set of procedures an organization follows to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels following a disruption.
- The Disaster Recovery Plan is the documented process to recover and resume an organization's IT infrastructure, business applications, and data services in the event of a major disruption.
- The Incident Response Plan is a set of instructions to help IT staff detect, respond to, and recover from security incidents.

An effective Business Resiliency Program should:

- Reasonably define the internal processes for responding to a cybersecurity event or disaster.
- Reasonably define plan goals.
- Define the documentation and reporting requirements regarding cybersecurity events and responses.
- Clearly define and describe the roles, responsibilities, and authority levels.
- Describe external and internal communications and information sharing, including protocols to notify plan sponsor and affected user(s) if needed.
- Identify remediation plans for any identified weaknesses in information systems.
- Include after action reports that discuss how plans will be evaluated and updated following a cybersecurity event or disaster.
- Be annually tested based on possible risk scenarios.

10. Encryption of Sensitive Data Stored and in Transit.

Data encryption can protect nonpublic information. A system should implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data at rest or in transit.

11. Strong Technical Controls Implementing Best Security Practices.

Technical security solutions are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. Best security practices for technical security include:

- Hardware, software and firmware models and versions that are kept up to date.
- Vendor-supported firewalls, intrusion detection and prevention appliances/tools.
- Current and regularly updated antivirus software.
- Routine patch management (preferably automated).
- Network segregation.
- System hardening.
- Routine data backup (preferably automated).

12. Responsiveness to Cybersecurity Incidents or Breaches

When a cybersecurity breach or incident occurs, appropriate action should be taken to protect the plan and its participants, including:

- Informing law enforcement.
- Notifying the appropriate insurer.
- Investigating the incident.
- Giving affected plans and participants the information necessary to prevent/reduce injury.
- Honoring any contractual or legal obligations with respect to the breach, including complying with agreed upon notification requirements.
- Fixing the problems that caused the breach to prevent its recurrence.

ONLINE SECURITY TIPS

You can reduce the risk of fraud and loss to your retirement account by following these basic rules:

• REGISTER, SET UP AND ROUTINELY MONITOR YOUR ONLINE ACCOUNT

- Maintaining online access to your retirement account allows you to protect and manage your investment.
- Regularly checking your retirement account reduces the risk of fraudulent account access.
- Failing to register for an online account may enable cybercriminals to assume your online identify.

• USE STRONG AND UNIQUE PASSWORDS

- Don't use dictionary words.
- Use letters (both upper and lower case), numbers, and special characters.
- Don't use letters and numbers in sequence (no "abc", "567", etc.).
- Use 14 or more characters.
- Don't write passwords down.
- Consider using a secure password manager to help create and track passwords.
- Change passwords every 120 days, or if there's a security breach.
- Don't share, reuse, or repeat passwords.

• USE MULTI-FACTOR AUTHENTICATION

- Multi-Factor Authentication (also called two-factor authentication) requires a second credential to verify your identity (for example, entering a code sent in real-time by text message or email).

• KEEP PERSONAL CONTACT INFORMATION CURRENT

- Update your contact information when it changes, so you can be reached if there's a problem.
- Select multiple communication options.

• CLOSE OR DELETE UNUSED ACCOUNTS

- The smaller your on-line presence, the more secure your information. Close unused accounts to minimize your vulnerability.
- Sign up for account activity notifications.

• BE WARY OF FREE WI-FI

- Free Wi-Fi networks, such as the public Wi-Fi available at airports, hotels, or coffee shops pose security risks that may give criminals access to your personal information.
- A better option is to use your cellphone or home network.

• BEWARE OF PHISHING ATTACKS

- Phishing attacks aim to trick you into sharing your passwords, account numbers, and sensitive information, and gain access to your accounts. A phishing message may look like it comes from a trusted organization, to lure you to click on a dangerous link or pass along confidential information.

- Common warning signs of phishing attacks include:
  - A text message or email that you didn't expect or that comes from a person or service you don't know or use.
  - Spelling errors or poor grammar.
  - Mismatched links (a seemingly legitimate link sends you to an unexpected address). Often, but not always, you can spot this by hovering your mouse over the link without clicking on it, so that your browser displays the actual destination.
  - Shortened or odd links or addresses.
  - An email request for your account number or personal information (legitimate providers should never send you emails or texts asking for your password, account number, personal information, or answers to security questions).
  - Offers or messages that seem too good to be true, express great urgency, or are aggressive and scary.
  - Strange or mismatched sender addresses.
  - Anything else that makes you feel uneasy.

- **USE ANTIVIRUS SOFTWARE AND KEEP APPS AND SOFTWARE CURRENT**
  - Make sure that you have trustworthy antivirus software installed and updated to protect your computers and mobile devices from viruses and malware. Keep all your software up to date with the latest patches and upgrades. Many vendors offer automatic updates.

- **KNOW HOW TO REPORT IDENTITY THEFT AND CYBERSECURITY INCIDENTS**
  - The FBI and the Department of Homeland Security have set up valuable sites for reporting cybersecurity incidents:
    - **https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view**
    - **https://www.cisa.gov/reporting-cyber-incidents**

WAREHOUSE EMPLOYEES UNION
LOCAL NO. 730 AND CONTRIBUTING COMPANIES'
PREPAID LEGAL SERVICES FUND

SECOND QUARTER 2021

ADMINISTRATIVE MANAGER'S REPORT

SECOND QUARTER 2021
CONTRIBUTIONS

EMPLOYER	RATE	HOURS	PARTICIPANTS	CONTRIBUTIONS
CANADA DRY	$0.07	103,065.84	218	$ 7,215
CANTEEN VENDING	$0.07	34,375.86	71	$ 2,406
EIGHT O'CLOCK COFFEE	$0.07	22,817.25	50	$ 1,597
GIANT 922	$0.07	4,600.00	9	$ 322
GIANT RECYCLING	$0.07	11,571.90	23	$ 810
GIANT WAREHOUSE	$0.07	117,479.18	209	$ 8,224
QUALITY CUSTOM DISTRIBUTION	$0.07	24,755.30	56	$ 1,733
UNION LOCAL 730	$0.07	1,280.00	3	$ 90
WASHINGTON FOOD	$0.07	1,871.00	4	$ 131
TOTAL		**321,816.33**	**643**	**$ 22,528**

AVERAGE HOURLY INCOME	$0.07

SECOND QUARTER 2021
EXPENSES

BENEFIT EXPENSES	AMOUNT	AVG. HRLY. COST	PERCENTAGE
STEVEN M. SINDLER	$ 17,774	$ 0.055	62.21%
SUBTOTAL	$ 17,774	$ 0.055	62.21%

OPERATING EXPENSES	AMOUNT	AVG. HRLY. COST	PERCENTAGE
ADMINISTRATION	$ 3,931	$ 0.012	13.76%
MISCELLANEOUS	$ 6,865	$ 0.021	24.03%
SUBTOTAL	$ 10,796	$ 0.033	37.79%

TOTAL EXPENSES	**$ 28,570**	**$ 0.088**	**100.00%**

MISCELLANEOUS

MISCELLANEOUS EXPENSES	AMOUNT	AVG. HRLY. COST	PERCENTAGE
ACCOUNTING	$ 4,300	$ 0.013	15.05%
ATLANTA CAPITAL MNGMT	$ 207	$ 0.001	0.72%
INVESTMENT MNGMT FEE	$ 385	$ 0.001	1.35%
IPS	$ 625	$ 0.002	2.19%
LEGAL	$ 1,264	$ 0.004	4.42%
MEETING	$ 32	$ -	0.11%
POSTAGE	$ 50	$ -	0.18%
PRINTING	$ 2	$ -	0.01%

TOTAL	**$ 6,865**	**$ 0.021**	**24.03%**

2021
QUARTERLY RECAP

	FIRST 2021	SECOND 2021	THIRD 2021	FOURTH 2021	TOTAL
CONTRIBUTIONS	$ 21,967	$ 22,528	$ -	$ -	$ 44,495
MISCELLANEOUS	$ -	$ -	$ -	$ -	$ -
INTEREST & DIVIDENDS	$ 5,712	$ 6,166	$ -	$ -	$ 11,878
TOTAL INCOME	$ 27,679	$ 28,694	$ -	$ -	$ 56,373
BENEFIT EXPENSES					
PROVIDER	$ 4,840	$ 17,774	$ -	$ -	$ 22,614
SUBTOTAL	$ 4,840	$ 17,774	$ -	$ -	$ 22,614
OPERATING EXPENSES					
ADMINISTRATION	$ 3,926	$ 3,931	$ -	$ -	$ 7,857
MISCELLANEOUS	$ 2,841	$ 6,865	$ -	$ -	$ 9,706
SUBTOTAL	$ 6,767	$ 10,796	$ -	$ -	$ 17,563
TOTAL EXPENSES	$ 11,607	$ 28,570	$ -	$ -	$ 40,177
TOTAL INCOME	$ 27,679	$ 28,694	$ -	$ -	$ 56,373
TOTAL EXPENSES	$ 11,607	$ 28,570	$ -	$ -	$ 40,177
SURPLUS (DEFICIT)	**$ 16,072**	**$ 124**	**$ -**	**$ -**	**$ 16,196**
AVERAGE HOURLY INCOME	$ 0.09	$ 0.09	$ -	$ -	$ 0.09
AVERAGE HOURLY EXPENSES	$ 0.04	$ 0.09	$ -	$ -	$ 0.07
SURPLUS (DEFICIT)	$ 0.05	$ -	$ -	$ -	$ 0.02
NUMBER OF PARTICIPANTS	641	643	0	0	642

2020
QUARTERLY RECAP

	FIRST 2020	SECOND 2020	THIRD 2020	FOURTH 2020	TOTAL
CONTRIBUTIONS	$ 33,005	$ 28,646	$ 23,387	$ 23,920	$ 108,958
MISCELLANEOUS	$ -	$ -	$ -	$ -	$ -
INTEREST & DIVIDENDS	$ 7,040	$ 6,850	$ 6,149	$ 6,277	$ 26,316
TOTAL INCOME	$ 40,045	$ 35,496	$ 29,536	$ 30,197	$ 135,274
BENEFIT EXPENSES					
PROVIDER	$ 21,681	$ 14,495	$ 6,851	$ 14,566	$ 57,593
SUBTOTAL	$ 21,681	$ 14,495	$ 6,851	$ 14,566	$ 57,593
OPERATING EXPENSES					
ADMINISTRATION	$ 5,686	$ 4,932	$ 3,918	$ 3,916	$ 18,452
MISCELLANEOUS	$ 2,603	$ 7,295	$ 16,050	$ 1,772	$ 27,720
SUBTOTAL	$ 8,289	$ 12,227	$ 19,968	$ 5,688	$ 46,172
TOTAL EXPENSES	$ 29,970	$ 26,722	$ 26,819	$ 20,254	$ 103,765
TOTAL INCOME	$ 40,045	$ 35,496	$ 29,536	$ 30,197	$ 135,274
TOTAL EXPENSES	$ 29,970	$ 26,722	$ 26,819	$ 20,254	$ 103,765
SURPLUS (DEFICIT)	**$ 10,075**	**$ 8,774**	**$ 2,717**	**$ 9,943**	**$ 31,509**
AVERAGE HOURLY INCOME	$ 0.09	$ 0.09	$ 0.09	$ 0.09	$ 0.09
AVERAGE HOURLY EXPENSES	$ 0.06	$ 0.07	$ 0.08	$ 0.06	$ 0.07
SURPLUS (DEFICIT)	$ 0.03	$ 0.02	$ 0.01	$ 0.03	$ 0.02
NUMBER OF PARTICIPANTS	947	823	661	652	771

SECOND QUARTER 2021
CONTRACT INFORMATION

COMPANY	CURRENT RATE	RATE EFF. DATE	CBA EXPIRATION
CANADA DRY[1]	$0.07	02-27-15	02-26-20
CANTEEN VENDING	$0.07	10-13-17	10-12-21
EIGHT O'CLOCK COFFEE	$0.07	10-01-04	07-17-27
GIANT 922	$0.07	04-28-11	06-25-22
GIANT RECYCLING	$0.07	08-01-04	06-25-22
GIANT WAREHOUSE	$0.07	05-30-04	05-15-27
QUALITY CUSTOM DISTRIBUTION	$0.07	07-28-16	07-28-25
UNION LOCAL 730	$0.07	05-30-04	Follows Giant Warehouse CBA
WASHINGTON FOOD	$0.07	11-01-06	10-31-21

[1]The agreement has been extended.

SECOND QUARTER 2021
UTILIZATION

STEVEN M. SINDLER

CATEGORY	TYPE	NEW CASES	ATTORNEY HOURS	PARALEGAL HOURS	HOURLY RATE	TOTAL CHARGES
01	ADVISE AND CONSULTATION	5	5.50	0.00	$ 140	$ 770
02	WILL	1	3.36	0.00	$ 140	$ 470
03	FAMILY	4	49.44	0.00	$ 140	$ 6,922
04	REAL ESTATE	1	6.00	0.00	$ 140	$ 840
05	TRAFFIC	2	45.06	0.00	$ 140	$ 6,308
06	CRIMINAL	0	17.60	0.00	$ 140	$ 2,464
07	JUVENILE	0	0.00	0.00	$ 140	$ 0
08	PROBATE/ESTATE	0	0.00	0.00	$ 140	$ 0
09	CIVIL PROCEEDINGS	0	0.00	0.00	$ 140	$ 0
TOTALS		13	126.96	0.00		$17,774

ALL HOURS	126.96
ADJUSTED HOURS	126.96
COST PER HOUR	$139.99

LEGAL

DELINQUENCY REPORT

As of June 30, 2021

NONE

Warehouse Employees Union Local No. 730
and Contributing Companies' Prepaid Legal Services Fund

INVOICES

September 1, 2021

Atlanta Capital Management Co., LLC

7/30/2021	Fee for investment services rendered through June 30, 2021	$ 157.00

Blank Rome LLP

8/4/2021	Fee for professional services rendered through July 31, 2021	$ 1,009.80
7/13/2021	Fee for professional services rendered through June 30, 2021	$ 594.00
6/2/2021	Fee for professional services rendered through May 31, 2021	$ 475.20

Investment Performance Services, LLC

6/7/2021	Fee for professional services rendered through June 30, 2021	$ 625.00

Novak Francella, LLC

7/27/2021	Fee for Audit services performed for plan year ended December 31, 2020	$ 1,000.00
6/14/2021	Fee for Audit services performed for plan year ended December 31, 2020	$ 4,300.00