KOSKIE MINSKY
JUSTICE MATTERS

MEMORANDUM

DATE: June 8, 2023

TO: Board of Trustees of the IUOE Local 793 Pension and Benefit Funds

FROM: Roberto Tomassini and Lauren Tarasuk

SUBJECT: Review - Global Benefits Cybersecurity Breach

This memo outlines the details of the Global Benefits cybersecurity breach involving the IUOE Local 793 Pension, Life and Health and the Group Legal Trust Funds (collectively, the "Funds") which occurred on January 16, 2023 and the actions taken to date, including the legal advice provided by Koskie Minsky to date.

The Cybersecurity Incident

On April 14, 2023, Michael Gallagher and the Fund's Board of Trustees (the "Trustees" or the "Board" received a letter from Global Benefits notifying them of a cybersecurity incident affecting the Global Benefits network.

The April 14th, 2023, letter indicated that Global Benefits first became aware of a cybersecurity incident as early as January 16, 2023. It was not until three months later on April 14th that Global Benefits made the Trustees aware of this incident. The letter indicated that Global Benefits was investigating this incident and that affected information included some or all of the following: name, address, date of birth, banking information and social insurance numbers or plan members and certain dependent information. Global Benefits did not at this time notify affected individuals and indicated they were in the process of finalizing logistics regarding that process.

After receiving the April 14th letter, Mike Gallagher and Joe Redshaw contacted Koske Minsky to discuss potential recourse available to the Trustees.

Koskie Minsky provided a legal opinion outlining the potential actions availability to the Trustees on April 20, 2023. The opinion outlined the legal merits of potential actions available to the affected members and the Trustees. The potential options included a complaint to the Privacy Commissioner of Canada filed by or on behalf of an affected individual.

The opinion noted that a civil remedy or court action had little prospect of success. Actions against organizations who are subject to hacking by third parties have faced significant challenges before the courts. These actions have been dismissed on the basis of a failure to prove that the organization perpetrated the breach and/or a failure to show compensable damages. We indicated that more information was needed quantify any damages experienced by the members or the Fund.

With instructions from the Trustees, we wrote to Global Benefits on April 25th, 2023. In that letter we expressed concern regarding the significant delay in notifying affected parties of the existence of a privacy breach. We asked that affected individuals be contacted immediately so that they

could take proactive measures to protect themselves of identity theft and fraud. We also asked that a 5-year credit monitoring protection and identity theft insurance of up to $2,000,000 be provided to each affected individual. We asked that Global Benefits report this breach to the Privacy Commissioner of Canada as there is a real risk of significant harm to affected individuals. We also requested that all personal information held be destroyed as Global Benefits was no longer a benefits administrator for the Trust Fund and had no legitimate purpose to continue to hold the Beneficiaries' data within reach of malicious actors on active networks.

We did not receive a timely response from Global Benefits to our request for information. As such, we wrote to Global Benefits again on May 15th, 2023. In that letter, we expressed concern that the lack of communication and transparency was deeply concerning to the Trustees. We reiterated that there exists a significant potential for fraud or identity theft that continues to grow unless proper mitigation measures were put in place immediately. The letter outlined that we expected to be provided with information concerning Global Benefits communications and remediation plans no later than May 18th, 2023. We warned that we would consider legal action if we did not receive a response.

After 10:00pm on May 18th, 2023, we received a response from legal counsel to Global Benefits. We were advised that affected individuals would receive letters in the coming week notifying them of the breach and offering credit monitoring for a 1-year period including insurance protection of $1,000,000. Despite our repeated requests Global Benefits refused to delete historical data noting that it was held to facilitate access or correction requests and response to any legal or regulatory proceedings. Global Benefits committed to endeavour to retain the information in a secure format off network.

Again, we wrote to Global Benefits on May 26th, 2023, taking issue with this position and indicating there was no legitimate purpose to continue to hold this data. It is deeply concerning that unnecessary information is being retained by Global Benefits for purposes that far exceed the purpose for which it was first collected. We also asked for further information concerning the type of data and information retained by Global Benefits and a copy of the retention schedule for the deletion of this information. We did not receive a response to this letter.

During the week of May 23rd, 2023, OEBAC provided a letter to each member advising them of the existence of the cybersecurity breach experienced by the former benefit plan administrator. We and OEBAC encouraged all members to take advantage of the 12-month credit monitoring service in order to receive protection against fraud or identity theft. The Trustees asked members to advise that they be informed of any loss as a result of the breach including any impact on credit scores.

Through escalating letters, the Trustees pressured Global Benefits to finally make its notification to affected members. On or about the week of May 29th, 2023, Global Benefits directly notified those Beneficiaries that Global Benefits determined were affected. The notification letter indicated that the cybersecurity breach involved personal information including names, addresses, dates of birth, banking information and social insurance numbers of former plan members as well as certain dependent information. The notification letter offered $1,000,000 insurance protection and credit monitoring for a 1-year period. This notification letter was provided over four months after Global Benefits first became aware of the cybersecurity breach.

Legal Recourse Available to the Board of Trustees

In our opinion dated April 20th, 2023, we reviewed potential avenues of recourse available to the Trustees. We also reviewed the applicable privacy frameworks including the statutory framework imposed by the *Personal Information and Protection of Electronic Documents Act* ("PIPEDA") and the treatment of privacy breaches by Canadian courts.

We advised that there are a number of narrow avenues available to claimants seeking recourse for privacy breaches. Ultimately, it is unlikely a court action will be successful without proof of loss or compensable harm.

Complaint to the Privacy Commissioner

The statutory framework in Canada, through PIPEDA provides individuals the ability to file a formal privacy complaint with the Privacy Commissioner of Canada. The Commissioner may investigate, make orders, prepare public reports and/or issue fines. Any complaint could allege that Global Benefits has failed to take actions required by legislation including notifying impacted individuals promptly and filing a report with the Privacy Commissioner. Due to the restrictive language in the legislation, it is unlikely that such a complaint could be initiated by the Trustees.

We have prepared a standard complaint form attached to this memo that can be sent to each member so that they can submit their own complaint to the Privacy Commissioner.

Civil Action

Further, we reviewed the treatment of privacy breaches by the Courts and advised that legal action is generally not successful unless damages or a form of loss can be established. There have been a few class actions in Ontario which have failed on the basis of a failure to show losses or damages. Cases where the organization did not directly interfere with the data, but were subject to third party hacking, known as "database defendant" cases.

A recent trilogy of cases from the Ontario Court of Appeal refused to certify class actions on the basis of a privacy claim. These "database defendants" or defendants who were victims of third-party hackers, could not meet the test to ground a claim of intrusion upon seclusion. They were not alleged to have been the actual party that "intruded" upon the individuals' "private affairs or concerns". The Court of Appeal refused to expand this tort to situations where the company fails to protect personal information from intrusion by others. The Court of Appeal also dismissed arguments that the organization acted recklessly or that they should be held vicariously liable for the actions of the third-party hackers.

In regards to cybersecurity, negligence can also be a difficult test to meet, as it also requires a compensable loss or proof of harm. Very few cases in this area have ever proceeded to trial and even fewer have resulted in damage awards.

In light of the requirement to show damages or compensable loss, the membership should be advised that any losses be communicated to the Trustees. If losses can be established, the Trustees may consider a claim for intrusion upon seclusion, negligence, breach of contract, breach of confidence and/or breach of fiduciary duty.