**MEMORANDUM**

TO: All Members of the Municipal Excess Liability Fund

FROM: Fred Semrau, Fund Attorney

 Dave Grubb, Executive Director

 Joe Hrubash, Executive Director

 Paul Shives, Safety Director

 Pauline Kontomanolis, Chief Accounting Officer

 Ed Cooney, Underwriting Manager

DATED: October 31, 2023

RE: MEL’s JCMI Banking Best Practices - Wire Transfers, ACH Payments (Automatic Clearing House) and Check Issuance.

Dear Public Entity Chief Financial Officer and Administrator:

Wire transfer fraud cyber-attacks cost U.S. businesses billions of dollars each year. A number of covered entities have experienced breaches to their information systems related to wire transfers with financial institutions that have resulted in losses that far exceed their crime and cyber insurance coverage. Many of these events could have been avoided by applying vigilant oversight and compliance with “best practice” guidelines.

The following is a list of best practices that the MEL JCMI requires the JCMI and MEL affiliated members to review and implement with their Administration, Chief Financial Officer, and lending institution to ensure all necessary protections are in place. **Failure to adhere to these required practices may lead to an increase in deductible, denial of claim or termination of coverage.**

**Best Practices for Wire Transfers and ACH Payments**

1. **Review contracts with financial institutions** – Your entity’s legal counsel must immediately review all agreements and be certain that the “presumptive liability” is placed on financial institutions that process wire transfers and ACH payments.

1. **Confirm receipt of Best Practices** – Verify that your Chief Financial Officer has reviewed each of these practices and provides specific “no exception guidelines” as to wire transfer and ACH payment policy and procedures.

1. **Include Best Practices in Annual Cash Management Plan** – Require that your Chief Financial Officer includes the entire Best Practices for Wire Transfer, ACH Payments, and Check Issuance protocol as part of the Annual Cash Management Plan pursuant to N.J.S.A. 40A:5-14, which is required to be adopted annually by the governing body.

1. **Establish specific wire transfer and ACH payment requirements** – Wire transfers payments are completed the same day while ACH payments take 1-2 business days for the transaction to be completed. Banking institutions have indicated that ACH payments are more secure than wire transfers. The following requirements must be part of your wire transfer and ACH payments policy:

1. Identify at least two authorized individuals in the covered entity who are authorized to execute and confirm wire transfers and ACH payments, respectively. The Official with financial administrative rights that is tasked with this process is required to have an appropriate level of responsibility. This official will set up the wire transfer or the ACH payment and the other official, also with an appropriate level of responsibility will authorize the release of the wire or ACH payment directly with the bank utilizing a separate platform other than the electronic platform utilized to initiate the wire, i.e., Telephone call or Phone Text, not an email on the same network.

1. Free form wire transfers and ACH payments must be blocked in the banking system. Only wire transfers where an approved wire or ACH template is authorized are allowed. Wire and ACH Template authorizations should go through the same approval process as noted in a. above, wherein Official 1 initiates and Official 2 confirms. Also, any changes to a template must be authorized using this same process. A wire transfer or ACH payment requires at least two forms of verification from the vendor bank before a transfer can be authorized. The verification should include: (i) multi-factor authentication for each authorized user; (ii) user verbal authorization and verbal confirmation using phone contact information on file, not the phone number in an email; and (iii) a limited email exchange to confirm the wire transfer. The additional factor(s) can be a text with a code sent to an authorized user’s smartphone, a hard token, or biometrics. The email exchange shall never contain specific information relating to the actual contents of the transfer.
2. For all wire/ACH transfer of funds, the following information is required:
3. Must create a template for all transactions.
4. Name of person spoken to, including the recipient vendor title and telephone number.
5. Name of the two individuals from the covered entity that verbally and in writing confirmed the authorization of the transfer, and the receiving bank information, including routing number, account number and dollar amount.
6. Confirming telephone call to vendor/receiving entity verifying transfer authorization, receiving bank information including routing number, account number and dollar amount.
7. Memorialization of the transfer and confirmation of completion of the transaction.
8. Exception to the above is when a recurring transaction with an established template is transacted, steps iii-v will not have to be completed.
9. Memorialization of each transfer/paymentmust be filed with the Chief Financial Officer/JIF treasurer and made available for audit.
10. A detailed description of all wire transfers and ACH payments must be filed with the Chief Administrative Officer and the Clerk.
11. Verbally confirm, within 24 hours, with receiving vendor/entity that the funds were credited to their account.
12. Entities are required to establish a policy restricting the frequency of wire transfers to infrequent or emergent matters, and real estate transactions, rather than for routine payments to vendors. The frequency of fraudulent transactions for wire transfers is far greater than for checks. Templates must be set up for wire transfers and ACH payments.

1. Entities are required to placing a dollar limit on wire transfers and ACH payments that is reasonable to your size entity but recognize when setting that limit that your coverage is limited to the maximum coverage of the crime policy and your entity will be responsible for any losses between the coverage limits and the wire limit you set.
2. Establish on-line banking alerts for all wires & ACHs changes to a template. The online banking policy must include a requirement that the wire/ACH is not released until the recipient of the alert approves it.
3. Covered entities are required to restrict all permissions on international wires. Authorized users are required to set up the restrictions on the banking institution’s on-line system.
4. Each Chief Financial Officer must utilize blocks and alerts in their banking system to ensure that any transactions not specifically authorized will be flagged by the banking system, and the Chief Financial Officer must authorize each flagged transaction. **The use of a Payee Positive Pay system for all checks and ACH transactions is required.** Additionally, daily review of overnight transactions and balances to identify any unusual transactions or events is strongly recommended.
5. Notify the bank and Chief Financial Officer/Treasurer/Responsible individual immediately if suspicious activity is detected.

**Cyber Insurance and Wire Transfers**

Generally speaking, wire transfer fraud is considered a theft and there may be limits of up to $250,000 depending on the incident. That leaves a potential gap for significant exposure beyond this coverage. There are important coverage contingencies in many policies, such as that the coverage will apply only if you “**properly verify the instructions to transfer such assets by following a prearranged procedure to authenticate the request**.” The bottom line is, insurers have been moving to restrict or eliminate coverage altogether, especially if proper controls are not in place. Many of the losses that we are seeing today throughout government agencies are easy to prevent, but also easy to create significant losses. Prudent controls must be implemented to protect our members and covered entities and minimize exposure, as well as to qualify for coverage.

**Conclusion**

In conclusion, we would ask that you thoroughly review this memorandum and ensure that your legal counsel, Administration and Chief Financial Officer have, at a minimum, adhered to these best practices.

If you have any questions, please do not hesitate to contact the undersigned.