REI - City of Philadelphia LOCs
Questions and Answers

Questions Related to General Fund/PAID

1. Please provide a list of third-party providers for Liquidity Facilities and Direct Placement Facilities. Please include the exposure amounts and number of facilities.
   Liquidity Facility/Direct Placement Facility Providers for Philadelphia General Obligation (GO) and General Fund-Supported debt, as of November 30, 2023:

Series	Principal Amount	Current Provider
GO 2009B	$100,000,000	Barclays
PAID 2007B-2	$46,575,000	TD Bank

2. Please provide the 12/31/2022 Audit or a Draft copy of the Audit for the Philadelphia Authority for Industrial Development (PAID).
   a. Please provide unaudited figures if the Audit/Draft Audit is not available.
   PAID is a conduit issuer on behalf of the City and is a Discretely Presented Component Unit in the City's financial statements.

3. Please provide a copy of the 9/30/2023 of the Quarterly City Manager's Report, if available.
   The 9/30/23 Quarterly City Manager's Report can be found here:
   https://emma.msrb.org/MarketActivity/ContinuingDisclosureDetails/P21326361

4. Please provide any updated information (Unaudited financials, notable information, etc.) for FYE 2023 that is available for distribution currently.
   The City's unaudited financials, the FY23 Annual Financial Report (AFR), can be found here:
   https://emma.msrb.org/MarketActivity/ContinuingDisclosureDetails/P21318660

Questions Related to Philadelphia Water Department

1. Can you share the most recent 3-year trend on delinquent accounts?
   The Water Department's cumulative collections of annual billings for Fiscal Years 2021, 2022 and 2023 were each, respectively, approximately 95.4%, 96.7% and 97.0%. Collections in Fiscal Years 2021 and 2022 were negatively affected by the moratorium on residential and commercial account shut offs implemented due to the COVID-19 pandemic. The moratorium on residential account shut offs was lifted on June 30, 2022, with the first residential account shut offs occurring the week of July 25, 2022. In Fiscal Year 2023, residential shut offs began on May 31, 2023 after the winter moratorium on residential account shut offs ended. In terms of commercial accounts, the Water Department ceased implementing the moratorium on shut offs for delinquent accounts implemented due to the COVID-19 pandemic in October of 2021. Since then, delinquent commercial accounts have been eligible for shut off on a rolling basis. There is no winter shut off moratorium in place for commercial accounts.

2. Can you provide un-audited financial statements for the fiscal year ending June 30, 2023? Please provide any updated information (Unaudited financials, collection rates, update to capital projects/plans notable information, etc.) for FYE 2023 that is available for distribution currently.

The Water and Wastewater System consolidated financial statements for the fiscal year ended June 30, 2023 are included in the City's FY23 AFR, which can be found here:
https://emma.msrb.org/MarketActivity/ContinuingDisclosureDetails/P21318660

3. Will the City consider a change to the Dealer for the Series B CP?
   The City is open to discussing such a change with the selected respondent.

4. Please provide a list of third-party providers for Liquidity Facilities and Direct Placement Facilities. Please include the exposure amounts and number of facilities.
   Liquidity Facility/Direct Placement Facility Providers for Philadelphia Water and Wastewater Revenue debt, as of November 30, 2023:

Series	Principal Amount	Current Provider
CP Series A	$125,000,000	Barclays
CP Series B	$125,000,000	RBC
CP Series C	$150,000,000	TD Bank

5. Please provide a copy of the 9/30/2023 of the Quarterly City Manager's Report, if available.
   The 9/30/23 Quarterly City Manager's Report can be found here:
   https://emma.msrb.org/MarketActivity/ContinuingDisclosureDetails/P21326361

Questions Related to Recent City of Philadelphia Data Breach

1. Please provide details on what occurred.
   In May 2023, the City of Philadelphia ("City") became aware of suspicious activity in its email environment. The City learned that it had been subject to a phishing attack, as a result of which a City email account subsequently was utilized by an unauthorized actor to send out further phishing emails. The City engaged a firm to conduct a privileged forensic investigation and to work with the City to confirm the event was contained.

   The investigation determined that between May 26, 2023 and July 28, 2023, an unauthorized actor may have gained access to nine (9) City email accounts and certain information contained therein. Also, on August 22, 2023, the City became aware that the at-issue email accounts include five (5) email accounts that may contain protected health information.

   The City is now conducting a comprehensive review of the potentially impacted email accounts to determine whether personal information or protected information was potentially affected. If so, the City will work to confirm the identities and contact information for potentially impacted individuals and provide notice via written letter.

   In the interim, to ensure compliance with applicable regulations while the data review is ongoing, on October 20, 2023, the City: (1) posted notice of the event on its website; (2) provided notice to the U.S. Department of Health and Human Services or "HHS"; and (3) provided notice to the media in the Philadelphia Inquirer. Once the data review is complete, the City will provide direct notice to individuals and businesses whose personal information or protected health information was potentially impacted, supplement its notice to HHS, issue updated website and media notices, and notify applicable state regulators and consumer reporting agencies, as required pursuant to applicable law or contract.

2. What steps are being taken to mitigate risk of breach in future?
   Upon becoming aware of the event, the City engaged third-party cybersecurity specialists to conduct a privileged forensic investigation into the nature and scope of the event, while also working with the City to ensure that its network and email environment were secure. The investigation included a review of the indicators of compromise ("IOCs") associated with the suspicious activity identified and a review of the City's entire email tenant for any other activity potentially associated with those IOCs. The investigation also included a review of all mailboxes to identify suspicious forwarding or other rules; any such rules were immediately disabled unless independently verified as legitimate by the user. The City also immediately reset passwords and revoked multi-factor authentication (MFA) sessions for any users whose accounts were identified as potentially impacted by this event. The City, with the assistance of a third-party vendor, also continues to monitor its endpoint detection and response (EDR) solution for anomalous behavior. Since July 28, 2023, the City has not identified any signs of suspicious or malicious activity in its network or email environment related to this event. Following the event, the City is also providing additional training to its employees and workforce members regarding cybersecurity, social engineering fraud, phishing attacks, and safeguarding protected information.

3. What potential financial impact to the City – or would the cost be insured under existing policy?
   The City is still in the incident response stage. However, the City has industry appropriate cyberliability insurance.

4. What are coverage levels of current policy?
   The City has industry appropriate cyberliability insurance.