State of North Carolina Supplemental Retirement Plans Group Trust

Board of Trustees Meeting

BNY Mellon Presenter
Matthew Coburn
Director, Relationship Manager
Agenda

• BNY Mellon Corporate Update
• Asset Servicing Overview
• 2022 Business Relationship Review
• Protecting SRP’s Assets and Data: A Cyber Security Overview
BNY Mellon Corporate Update

BNY MELLON 4Q22

$44.3 trillion
assets under custody and/or administration\(^1\)

$1.8 trillion
in assets under management\(^2\)

- BNY Mellon’s assets under custody and administration (AUCA) decreased by -5.14% from Q421 to Q422; whereas assets under management decreased by -25% during same period.
- Declines are indicative of the 2022 market; however, disparate rates of decline are indicative of strength and growth!
- BNY Mellon winning business at 3:1 ratio over primary competitors; revenues +15%, expenses -1%.

<table>
<thead>
<tr>
<th>EMPLOYEE GROWTH</th>
<th>CREDIT RATING</th>
<th>STRATEGIC PRIORITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global workforce increased 5.4% since Q421 (50,000+ employees)</td>
<td>Highest credit rating amongst custodian banks</td>
<td>Continued focus on data &amp; digital strategy; investing in best-in-class partners and technology</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CREDIT CATEGORY</th>
<th>Moody's</th>
<th>S&amp;P</th>
<th>Fitch</th>
<th>DBRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long-term senior debt</td>
<td>A1</td>
<td>A</td>
<td>AA-</td>
<td>AA</td>
</tr>
<tr>
<td>Subordinated debt</td>
<td>A2</td>
<td>A-</td>
<td>A</td>
<td>AA (Low)</td>
</tr>
<tr>
<td>Preferred stock</td>
<td>Baa1</td>
<td>BBB</td>
<td>BBB+</td>
<td>A</td>
</tr>
<tr>
<td>Short-term debt</td>
<td>P-1</td>
<td>A-1</td>
<td>F1+</td>
<td>R-1 (Middle)</td>
</tr>
<tr>
<td>Outlook</td>
<td>Stable</td>
<td>Stable</td>
<td>Stable</td>
<td>Stable</td>
</tr>
</tbody>
</table>
A Comprehensive Suite of Global Custody Services…

Our core custody services are designed to optimize and streamline your investment process.

Services are supported by integrated technology tools to simplify your workflow.
Our core portfolio services are integrated with our custody platform to provide seamless processing and operational efficiencies.

**INSTITUTIONAL ACCOUNTING**
- Integrated Accounting Platform (IAS): Inputs from cash processing, custody, recordkeeping, funds, private investments, corporate events, pricing, etc.
- Outputs timely and accurate daily and monthly net asset values for all plan types
- General Ledger Based Accounting: Integrated ledger, trial balance and accounting journal supporting all accounting transactions
- Supports complex unitized plan accounting structures within the same platform

**RECORD KEEPER SUPPORT**
- Standard scalable processes and controls across record keepers
- Daily automated transmissions Between BNY Mellon and Empower
- Automated unit reconciliation between BNY Mellon and Empower
- Dedicated recordkeeper liaison for Empower
- Project Manager for Any Plan Changes to ensure seamless integration and processing for plan

**SMART ALLOCATOR**
- Using the plan recordkeeper’s files, Smart Allocator automatically allocates and rebalances the fund activity based on the previous day’s cash flows while using the valuation fluctuation and the fund target percentage
- Minimizes trading activity, thereby minimizing transactional costs
- Fully-automated solution reducing time and processing risk
- Balances out the shifts due to market fluctuation

**PERFORMANCE MEASUREMENT**
- Performance measurement platform (RAM) integrated with the IAS accounting platform for automated data delivery
- Produces daily and monthly performance measurement
- Analyze portfolio data characteristics in a myriad of ways with daily and monthly portfolio analytics
- Custom benchmark reporting to measure portfolio performance against peers and benchmarks
- Compliance Monitoring ensures that SRP’s investments comply with state mandated investment guidelines

**FOREIGN EXCHANGE**
- Fully automated FX standing instructions for all security and corporate action related transactions
- FX Overlay providing a fully outsourced service designed to manage and mitigate currency risk for our clients
- Direct access to FX Dealing desk and suite of e-commerce provision for clients seeking negotiated FX solutions

**CASH MANAGEMENT**
- Daily automated sweep of uninvested cash into BNY Mellon’s low fee EB Temporary Investment Fund (EBTIF)
- Late money cash deposits on BNY Mellon’s secured balance sheet (i.e. late money sweep)
- Daily automated sweep of uninvested cash into BNY Mellon’s low fee EB Temporary Investment Fund (EBTIF)
- Late money cash deposits on BNY Mellon’s secured balance sheet (i.e. late money sweep)
2022 Business Relationship Review
Strengthening for the Future

Custody Agreement Amendments
- Contract term alignment w/ existing DST contracts
- Hong Kong Stock Connect opening for China A share investments
- Information security breach protocol enhanced to 24 hours notification time

BNYM News
- Relationship Oversight Change (Garibaldi to Coburn)
- BNYM CEO Todd Gibbons retires; Robin Vince takes helm
- BNYM outsources class actions filing to FRT
- BNYM partners w/ Xceptor for enhanced tax services experience

On-going Initiatives
- Continued Smart Allocator rollout w/ quarterly rebalancing and updates to the custody fee processing
- Participation in implementation of GlobeTax as supplemental tax services provider
- NEXEN / Instruction Capture Training
Cybersecurity & Business Resiliency
Executive Summary

• Protecting the confidentiality, integrity and availability of our clients' information is paramount to our business and our clients—and part of our corporate values.

• As a major financial services firm, BNY Mellon is very aware of recent cyber attacks impacting our industry—from ransomware and distributed denial of service (DDoS) attacks to advanced persistent threats (APTs) and system infiltrations via third-party suppliers.

• BNY Mellon has continuously invested in its information protection and cybersecurity programs for many years, developing its people, processes, and technology.

• Our cybersecurity strategy is fully integrated with our business, employing multiple layers of controls to protect the security of our clients' information and technology assets. Our cybersecurity services model organizes and aligns our program against leading standards such as ISO 27001/2 and the NIST Cybersecurity Framework.

CTOC: Cyber Technology Operations Center
About CTOC

**Predict. Identify. Resolve.**
This is the driving mantra behind BNY Mellon’s Cyber, Technology, and Operations Center (CTOC).

The CTOC was built to bring business and technology experts into one room (virtually since the onset of the pandemic) to reduce the time to identify and resolve issues and deliver next-level resiliency using:

- Advanced monitoring
- Rapid response
- Seamless processes
- Relentless client focus

**Virtual CTOC:** Since the onset of the pandemic, employees have been working remotely. BNYM teams across Technology, Cyber and Operations have been collaborating seamlessly in Virtual CTOC, leveraging the same tools and technology used in CTOC.
Cyber Attackers are Diverse and Use a Wide Range of Tools to Bypass Even the Most Sophisticated Defenses

**Nation State Actors**
- N. Korea, Russia, China
- Intellectual property
- Cripple/disrupt services

**Cyber Criminals**
- Ransomware
- Financial Gain
- Intellectual Property

**Insiders**
- Financial Gain
- Disrupt Services
- Destroy Data

**Hacktivists**
- Disrupt Services
- Further Cause
- Reputational Loss

**Recreational Hackers**
- Disrupt Services
- Financial Gain
- Gain Reputation

### How They Do It
- **Social Engineering**
- **Insider-Coordinated Breach**
- **Malware Infection Through Email**
- **Exploit Internal and Third Party Vulnerabilities**
- **Web Facing Application Vulnerabilities Compromised**
- **Credential Theft Through Phishing**
- **Anonymous Whistleblower, e.g., Wikileaks**
- **Distributed DoS Attacks and Ransom**

### What They Target
- Customer account information and credentials
- Potentially sensitive information such as investment strategies
- Confidential correspondence
- Loss of confidence in financial institution
- Disruption of services
- Destruction of data and IT assets
- Customer account information and credentials
- Potentially sensitive information such as investment strategies
- Confidential correspondence
- Loss of confidence in financial institution
- Disruption of services
- Destruction of data and IT assets
Cyber Threat Landscape: What’s New?

What changes have we seen in the cyber threat landscape over the last year?

**Advanced persistent threats or nation state sponsored destructive malware**

- These types of attacks have garnered more attention due to the capabilities of the threat actor as well as the time and money that can be spent on a potential target
- This may not be the most likely attack and varies depending on the geopolitical climate

**Spear phishing**

- This remains the most common attack vector and is potentially very damaging to a target

**DDoS (Distributed Denial of Service)**

- While these attacks have become less common, the proliferation of Internet of Things (IOT) devices and the myriad of tools available to execute DDoS have renewed focus on this type of attack
BNY Mellon Approach to Cybersecurity

Our framework has allowed us to establish a multi-layered control infrastructure and a service-based model with built-in redundancy and checks.

- **IDENTIFY**
  - Risk Management, Information Classification, Continuous Asset Discovery, Governance and Oversight

- **PROTECT**
  - Penetration Testing, Infrastructure, Encryption for Emails and Devices, Malware Protection, Vendor Risk Management, Web Proxy & Network Access Controls, Awareness & Training

- **DETECT**
  - Fraud Prevention & Response, Cyber Analytics, Threat Intelligence, Partnerships & Data Sharing, Insider Threat Program, Predictive Controls

- **RESPOND & RECOVER**
  - Incident Management, Crisis Management, Fraud Remediation & Recovery, Legal, Network Forensics, Host Forensics, Media Relations
## Threat Intelligence Sources

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
<th>Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS-ISAC</td>
<td>Daily threat summaries, individual partner organization reports, indicators of compromise</td>
<td>Global – Financial Sector</td>
</tr>
<tr>
<td>US Government</td>
<td>Finished intelligence assessments, analysis on APT actors of concern, ability to request further information on current and future threats or campaigns</td>
<td>Domestic Threats and APT Activity</td>
</tr>
<tr>
<td>Paid Threat Intelligence Vendors</td>
<td>Tailored priority intelligence requirements on key threats affecting BNY Mellon and the US FSS, daily threat reports, and detailed analytic studies on topics of direct impact</td>
<td>Global Targeted to BNY Mellon Requirements</td>
</tr>
<tr>
<td>Security Researchers</td>
<td>Open source provided threat studies of broad applicability and interest to the US FSS</td>
<td>Global – All Sectors</td>
</tr>
<tr>
<td>Open Source Data and Social Media</td>
<td>Current information and data on active incidents, emerging campaigns, and ideologically motivated hacktivist or cyber criminal actions</td>
<td>Global – All Sectors</td>
</tr>
</tbody>
</table>
### Participation in Industry Forums

<table>
<thead>
<tr>
<th>Organization Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Industry Shared Assessments Program (FISAP)</td>
</tr>
<tr>
<td>Financial Services Information Sharing and Analysis Center (FS-ISAC)</td>
</tr>
<tr>
<td>Financial Services Sector Coordination Council (FSSCC)</td>
</tr>
<tr>
<td>Financial Services Information Exchange (FSIE)</td>
</tr>
<tr>
<td>Internet Security Alliance (ISA)</td>
</tr>
<tr>
<td>Infragard</td>
</tr>
<tr>
<td>Information Security Systems Association (ISSA)</td>
</tr>
<tr>
<td>Information Systems Audit and Control Association (ISACA)</td>
</tr>
<tr>
<td>Information Security Forum (ISF)</td>
</tr>
<tr>
<td>Multi-State Information Sharing and Analysis Center (MS-ISAC)</td>
</tr>
<tr>
<td>New York Electronic Crimes Task Force (ECTF)</td>
</tr>
<tr>
<td>BITS (Technology arm of the Financial Services Roundtable)</td>
</tr>
</tbody>
</table>
ISO 27001 Certification

BNY Mellon has achieved ISO 27001 Certification of its Information Security Management System Framework, including but not limited to:

- Antivirus Management
- Asset Management
- Backup & Restoration Management
- Capacity Management
- Change Management
- Compliance
- Cryptography
- Data Centers
- Desktop Security
- HR Security
- Incident / Problem Management
- Information Security Continuity
- Information Security Policies
- Information Systems Audit Controls
- Logging & Monitoring
- Network Devices
- Organization of Information Security
- Patch Management
- Physical Security
- Remote Access Management
- Supplier Management
- Transport and Storage of Media
- User Access Management
- Vulnerability Management
Business Continuity

Our business continuity program establishes plans to promptly and effectively respond to and recover from business disruptions, facilitate service continuity, and continuously improve our resiliency.

- **Planning**
  - **Business Impact Analyses** identify and prioritize business services and processes based on disruption impact.
  - Our **plans** establish how each business unit and supporting technologies will respond to and recover from disruption events.

- **Recovery Solutions**
  - Our recovery solutions help mitigate the impacts stemming from business disruptions.
  - Using an **all-hazards planning approach**, solutions respond to any combination of workforce, technology, facility & supplier loss.
  - The solutions include **alternate sites, remote work, and cross-regional recovery**.

- **Training**
  - All BNY Mellon employees complete **annual business continuity training** including online courses, presentations, and facilitated tabletop simulations.
  - Employees with business continuity responsibilities are regularly educated to be able to react, respond and recover in line with our plans and protocols.

- **Testing**
  - We test our recovery strategies on a regular basis to confirm they are viable and sustainable.
  - Tests include recovery of facilities, applications, business services, focus on notifications and call-trees, and enterprise-wide exercises.
  - We leverage the test results to improve the business resilience.