*Quarter Ended June 30, 2024*

# Deferred Comp/NYCE IRA

# UPDATE

**The Newsletter for the 457 and 401(k) Plans and the NYCE IRA**

## In This Issue:



## Account Security & Cybersecurity Education

The Deferred Compensation Plan recognizes the importance of safeguarding your financial accounts and your personal information against the ongoing risk of fraud, cyber threats, and other unauthorized activity. We believe that keeping your account secure is a mutual responsibility, that means you play an important role in this process. Remember that you are your own first line of defense when it comes to protecting your accounts and identity. Below are some general tips on keeping your online accounts safe:

1. Register your account online: If you don't someone else may - to your detriment!
2. Get payments from the Plan strictly as direct deposits. Avoid checks.
3. Review your account information on a regular basis and keep your contact information and beneficiary information current.
4. Promptly report any suspected identity theft or unauthorized activity.

### When you register your account online

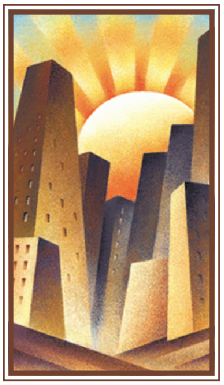
- Create a unique username
- Use your cell phone number instead of your email address for authentication purposes: If someone tries to access your account, you will receive automatic notification.

### General password/PIN security

- Use a unique password/PIN for each site where you maintain an account and regularly update your passwords/PINs. Never use your date of birth or Social Security number as your password/PIN.
- Don't allow social networking sites to memorize your passwords/PINs.
- Don't share your password/PIN or answers to security questions with anyone. In general, your account numbers, PINs, passwords and personal information are the keys to your accounts.
- The strongest passwords are comprised of a chain of unrelated common words.
- Enroll in Voya Voiceprint, Voya's voice biometrics program.

### Beware of fraudulent emails or phishing

- Be suspicious of emails asking for your confidential information and never provide credentials.
- Look out for red flags such as urgent requests, unknown email addresses or discrepancies between actual and displayed hyperlinks.
- Be aware that fraudulent emails can appear to come from a business that you are working with. Always review sender name, email addresses and urls to ensure they are from legitimate sources.
- The Plan's recordkeeper, Voya, will never ask you for your personal information by email.



## Monitor your accounts frequently

- Monitor your financial accounts frequently, and be sure to look for unusual transactions. Download the Plan's mobile app; a secure, easy and convenient way to access and manage your account all in one place.
- Sign up for electronic delivery of important documents to get quicker notification of account activity.
- Immediately open your statements and confirmation letters to verify all activity. If you notice anything suspicious, call the Plan's Client Service department immediately at (212) 306-7760.

## Take care of your computer and mobile devices

- Update your computer by installing the latest software and patches to prevent hackers or viruses from exploiting any known weaknesses.
- Install and update anti-virus software to protect your computer and to prevent hackers from installing malware or viruses on your computer.
- Check your operating system to see if firewalls are included. If not, be sure to install a firewall to regulate the flow of information between computers.
- Use only programs from a known, trusted source.
- Backup your important files on a regular basis and store the backups in a secure place.

## What to do if you are a victim of a data breach

1. Consider changing any PIN or password used to access all your financial accounts, especially if the PIN or password contains any part of your Social Security number or date of birth.
2. Sign up for account alerts or electronic delivery of notices from your financial institutions if available.
3. Order copies of your credit reports from the three national credit-reporting agencies, Experian, Equifax and TransUnion. Then, look for accuracy or indications of fraud, such as unauthorized applications, unfamiliar credit accounts, credit inquiries, defaults and delinquencies that you did not cause.

## What to do if your identity has been stolen

1. Visit the federal government's website identitytheft.gov for detailed instructions on how to report and recover from identity theft. This site provides streamlined checklists and sample letters to guide identity theft victims through the recovery process.
2. Contact the Plan and your other financial institutions and credit card issuer(s) to inform them that your identity has been stolen.

# Federal Trade Commission Guidelines for Protecting Your Data

## Don't send money to someone you don't know

This may seem like a "no brainer" but a stranger in this sense also includes a merchant you've never dealt with before or someone you've met online that is asking for money. If you want to make an online purchase, look for payment options that offer protection like a credit card or PayPal. Again, avoid a wire transaction or sending cash.

Don't respond to messages that ask for personal or financial information. Whether the message comes as an advertisement, an email, or a phone call, never give personal or financial information. If you receive a message that has you concerned, call the numbers on your credit card or statements and speak with an employee to make sure the request is legit.

## Don't play a foreign lottery

You may have already received a message claiming "You've Won!" and then be asked to simply pay "taxes," "fees," or "customs duties" in order to collect your prize. If you send money, you may never get it back – and it's actually illegal to play a foreign lottery.

## Read bills and statements regularly

A dishonest merchant can sometimes bill you for a monthly "membership fee" or other goods or services that you didn't authorize. Scammers can also steal your information and run up charges. By staying on top of your bills and statements, you'll be able to quickly notice charges you don't recognize. If you do, call your bank or credit card issuer immediately.

## Give to an established charity

When a natural disaster, or any unexpected crisis strikes, new charities may be established to serve the immediate needs of victims and survivors. Many times, these charities are legit, however, there could be someone using this unfortunate incident to their benefit. These con artists intend to swindle the public by setting up a shell organization to steal your money. Before making a donation, check out ftc.gov/charity for more information on the organization you're interested in.

## There's no such thing as a sure thing

If it sounds too good to be true, 99% of the time it is! Pitches that force you to "act now," guarantees a big profit, promises little or no financial risk, or demands you send cash immediately, should be reported to the FTC so they can investigate. You can also contact your state's Attorney General to see if they have any information on the person(s) contacting you. Snopes.com is another resource for checking if the offer you just received is legit.

## Know the person you are dealing with and where an offer is coming from

Try to find a seller's physical address (not just a Post Office Box) and phone number. With Voice-Over-Internet Provider (VoIP) and other web-based systems, it can be difficult to trace where a phone call is coming from. Always research the company; check out their website and search for reviews of the company. Also, the Better Business Bureau website at bbb.org can provide additional information.

## Don't dismiss your feelings

A lot can be said for your gut instincts – if something doesn't have the look of a real business or just doesn't feel right, don't dismiss that feeling. It's never a bad move to do a little research, whether it's simply asking friends or family what they think or digging a little deeper online or at the library. Protecting yourself from fraud is important and the old adage "better safe than sorry" can go a long way!

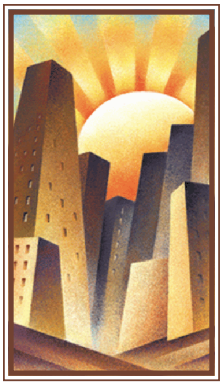
Remember…The FTC is here to protect the consumer. To file a complaint or get free information on consumer issues, go to ftc.org, call 877.FTC.HELP (877.382.4357, TTY: 866.653.4261).

Source: "Putting a Lid on International Scams: 10 Tips for Being a Canny Consumer"

### Additional Items

The Deferred Compensation Plan/NYCE IRA 2023 Annual Comprehensive Financial Report is available in the Forms & Downloads section on the Plan's website at nyc.gov/deferredcomp.

Download the Plan's mobile app available for iOS and Android. Search your app store for "NYC DCP". You can access your account through the mobile app to view fund information and performance, get your account details and perform transactions. Log into your account through the mobile app with the same username and password you established when accessing your account through the Plan's website.



# Direct Deposit

## The #1 best way to safeguard your financial accounts and personal information!

Whether you are going to receive a disbursement from the Plan as a distribution payment, a loan or hardship request, setting up direct deposit will ensure that you receive your payment quickly and securely.

## Direct deposit is fast, convenient and secure!

Just like with direct deposit of your net pay from the City, your Deferred Compensation Plan payments are electronically transferred into your bank account, so there's no more:

- waiting for your check to arrive in the mail
- waiting in line at the bank or
- worrying about the risk or hassle of replacing a lost or stolen check.

And…direct deposit is good for the environment because it reduces paper and ink use.

## Sign up for direct deposit today!

To get started, simply complete the Deferred Compensation Plan Direct Deposit Form, available from the Forms and Downloads section of the Plan's website at nyc.gov/deferredcomp. You only have to sign up once. All future Plan disbursements will be sent via direct deposit to the bank account you designated on your form.

It couldn't be simpler or greener!





The City of New York

Deferred Compensation Plan/NYCE IRA
A division of the
Mayor's Office of Labor Relations'
Employee Benefits Program
(212) 306-7760

Eric L. Adams
Mayor
City of New York

Renee Campion
Commissioner
Office of Labor Relations

nycdcp

1-888-DCP-3113
(outside of NYC)
nyc.gov/deferredcomp

NYCE IRA Our only interest is your interest℠

1-888-IRA-NYCE
(outside of NYC)
nyc.gov/nyceira