

### Account Theft Offers Reminder for Safeguarding Information

An identity theft that impacted an investor who held a retirement account with J.P. Morgan & Co. has been making headlines recently.

As reported, the victim's 401(k) account was electronically liquidated after his account was illegally accessed over the Internet. The proceeds of the victim's account were wired directly to a private checking account, which was set up when the account was illegally accessed. The distribution requests reportedly were made by someone who had the correct user ID and password to access the account. No additional information on how this person obtained the correct account access information was included in any reports on this incident.

We can certainly understand the concern this event may cause you or your participants. Maintaining the safety and privacy of participant data is critical and NYLIM Retirement Plan Services has many procedures in place to help safeguard this information. For example, we do not allow participants to set up or link to private checking accounts for total distributions. Additionally, we do not allow wire transfers for online distributions. All distribution checks are mailed to the participant's address of record only.

In the incident described above, J.P. Morgan was able to recover the stolen funds. Questions have been raised about what would have happened if the funds had not been recovered. Under ERISA, any *authorized* individuals who handle funds must be bonded and that bond will cover loss due to fraud or theft. However, plan sponsors and participants should be aware that fraud by an *unauthorized* person due to actions by the participant (e.g., giving their PIN to another individual or accessing their account in a non-secure environment) may not be covered by insurance.

This incident should serve as a reminder for Internet users to know and understand their responsibility for safeguarding their ID and password information and their personal data on their computers. NYLIM recommends the following safeguards for anyone who maintains or accesses financial information online.

**Protect your credentials:** Do not write down or share IDs or passwords with anyone. Make your user ID and password more complex (e.g., a random association of letters and numbers rather than birthdates or nicknames). Avoid using your Social Security number wherever possible.

**Protect your computer:** Configure your computer to reduce the likelihood of hacking by  
Automating the installation of system updates and  
Installing anti-virus and anti-spyware software and automate installation of their updates.

**Protect your network:** If you have a wireless network, set up security features such as WPA to secure the communication and MAC filtering to control which machines can access your network.

The safeguarding reminders listed above will be posted to participants' mailboxes on the Benefits Complete website.

