
# Ensuring Public Pension Trust and Security

## INTRODUCTION

As global markets remain unsteady and the wave of baby boomer civil servant retirements continues, ensuring the trust and security of America's public pension systems becomes even more paramount. Pension administrators have long anticipated the trend of baby boomer retirees and the need for more modern core systems and have been upgrading their platforms accordingly with enhanced member self-service, digital experiences, and targeted member campaign management. However, pension systems' increased digital footprint along with their significant assets ($4.5 trillion, with $323 billion in annual benefit distributions)[1] have made them attractive targets for cyber attacks and identity fraud. To combat this ongoing problem, security professionals can employ more advanced measures for comprehensive cybercrime management, while using CRM and targeted campaigns to educate members on fraud prevention and security efforts, to ensure greater member trust.

## BALANCING USER EXPERIENCE AND SECURITY

Pension members continue to benefit from pension systems' ongoing digital transformations. Omnichannel self-service and advanced member experiences have provided members with more 24/7 administrative capability and personalized engagement throughout their digital journeys. But the proliferation of member self-service combined with the growing trend of remote work has presented cybercriminals with greater opportunities to commit fraud and cyber theft. Public employees' plans have a "unique vulnerability" because so much of their personal data is publicly available on the internet due to their government employment.[2] This data can then be used to narrow down the remaining information required to take over their retirement accounts by stealing their identities.[3] Also of concern is the growing prevalence of insider fraud among public pension staff and external partners, such as IT consultants, payroll providers, and actuaries. To prevent these situations, pension administrators must remain alert to suspicious activity and consistently improve existing measures by strengthening current defenses or developing effective alternatives. Modern policy administration systems (PAS) must provide enhanced auditing and intelligence in helping administrators monitor account activity.

### Common Cybercrimes and Prevention

The most widespread forms of cybercrime include phishing and ransomware attacks. Most incidents start with a simple phishing email that results in a staff member acting on the "request," leading to a compromise of member account information.[4] This leads to account takeovers, ransomware incidents, and funds theft. Multifactor identification, a verification process that includes member username and password, token, or authenticator app, is rapidly becoming a standard authorization strategy to combat phishing and member fraud.

To combat "insider crimes," Artificial Intelligence (AI) has been particularly effective in detecting anomalies by using statistical models or rules to compare transactions and performing audits at scale with increasing accuracy. AI can detect suspicious activity by analyzing all transaction-related information and the supporting data to determine validity, and by verifying the names of members against those of payment recipients, so that proxy accounts cannot be used for embezzlement. AI can also force dual control measures that require more than one employee to perform a task to ensure that proper protocols are followed.

A particularly effective method of fraud prevention has been the widespread adoption of Know Your Customer (KYC) guidelines, which have become instrumental in modern PAS for customer verification and validation. KYC policies incorporate identification procedures, transaction monitoring, and overall risk management to identify suspicious elements early in the member-pension system relationship.

## STRENGTHENING MEMBER TRUST

Pension cybertheft not only robs members of their pension funds but of their trust in their fund administrators' security standards and protocols. To bolster member confidence, pension systems can use CRM for targeted campaigns to not only inform members about their ongoing security efforts and improvements, but also educate them about being vigilant to potential scams and security breaches.

## CONCLUSION

As many U.S. public pension systems continue their digital transformations, it is an opportunity for administrators to expand their security protocols while reassuring their members of their dedication to their funds' protection and preservation. Using CRM to continually educate members about how to avoid cyber attacks and identity theft should be a standard practice among system administrators so that members will have more of a stake in protecting their pension accounts. Despite public pensions' unique risks, they can be reframed as opportunities to develop air-tight security measures and stronger relationships with members for pension systems' greater good and welfare.

## ABOUT VITECH

Vitech is a global provider of cloud-native benefits and investment administration software. We help our Insurance, Retirement, and Investment clients expand their offerings and capabilities, streamline their operations, gain analytical insights, and transform their engagement models. Vitech employs over 1,600 professionals, serving the world's most successful insurance, retirement, and investment organizations. An innovator and visionary, Vitech's market leadership has been recognized by industry experts, such as Gartner, Celent, Aite-Novarica, and ISG. For more information, please visit vitechinc.com.

1 U.S. Census Bureau Data, Public Plans Data, December 2021
2 "How Plan Sponsors Can Combat Cybercrime," PlanSponsor, October 2022
3 Ibid.
4 "Phishing and Ransomware Risks on the Rise for Pension Funds, Says Expert," Benefits Canada, Sept. 2, 2021