M E M O R A N D U M

TO: All Retirement Boards

FROM: John W. Parsons, Esq., Executive Director

RE: PROSPER Security Update

DATE: June 26, 2020

PERAC's IT department recently ran a simulated phishing security test to determine what the PROSPER application vulnerability would be if a real phishing attack were to happen to our users. You may have received an email from "Employee Appreciation PERAC.perks@starbuckscommunityrewards.com" with a subject "Thank you from PERAC."

[redacted] While this was a simple simulated phishing attack using an incentive, phishing attacks can be much more sophisticated and difficult to detect. Phishing, the process of trying to gain access to sensitive information such as usernames, passwords, and other personal identifiers by pretending to be a credible entity, is usually done by sending out bulk emails to try to avoid spam filters.

Cybercrime is getting more serious by the month. Hackers are getting smarter about tricking people into clicking on fraudulent links or opening up malicious attachments in emails. It can happen to you personally on your own computer and email as well.

Because of this, our agency has decided to offer comprehensive security awareness training. Security is everyone's job and you are the last line of defense in keeping sensitive information safe and protect against cybercrimes. We know some agencies already provide their staff and board members with training. We will soon offer training to those PROSPER users who are not already receiving security

training. Keeping our retirees' information safe requires everyone who has access to PROSPER to be aware of cyber security threats and do their part to protect the information.

In addition, PERAC is investigating additional security controls to reduce the risk of an actual phishing attack in the future. These additional security controls will require an extra step to login to PROSPER. We also suggest asking your IT department what processes they have in place to protect your email from such an attack. If you are using a personal computer or device to access PROSPER, you are expected to have the latest security patches and up-to-date anti-virus software running on your device.

Once we schedule the training, we will send you an email invitation to take this training. In addition to security training, we will also send out simulated phishing tests regularly so you can practice the skills you will learn as part of your training. Please forward any concerns or questions about PROSPER security to: PER-ProsperHelp@per.state.ma.us.

Thank you for your cooperation.