1 ADP Boulevard
Roseland, N.J. 07068

Date: August 5, 2019
From: ADP Global Security Organization
Subject: Phishing Campaign: “Action required: confirm your email" // "ADP updated policy: Action required"

ADP has received reports regarding fraudulent emails being sent to ADP clients from email addresses that have the following format: Payroll Security Workforcenow [donotreply<AT>semnurpharma[.]com] or Workforcenow [freydd.rer<AT>poconosprings[.]org] with the following subject lines : “**Action required: confirm your email**" or "**ADP updated policy: Action required**". These emails instruct the recipient to click on a link in order to verify their email address.

These emails do not originate from ADP and our analysis has revealed that they may contain malicious content. We’re working with our fraud prevention team and anti-phishing vendor to address this incident. Please see the examples below which may vary in content and sender.

How to Report a Phishing Email

Be alert for this fraudulent email and follow the instructions below if you receive any suspicious email.

- **Do not click on any links or open any attachments** within the message.
- Forward the email as an attachment to abuse@adp.com, then delete it.
- If you clicked any link or opened an attachment in the email, immediately contact your IT support.

The ADP Global Security Organization continues to actively monitor this situation. Clients are encouraged to visit our website at www.adp.com/trust to learn more about how ADP protects data, and how clients can help protect themselves. Protecting our clients and their data from malicious activity is a top priority for ADP.