

ADP has identified a phishing attack targeted at ADP clients and others. The initial attack was made on a third-party "business contact" information system that ADP uses to hold client and other third party information, including names, addresses, email addresses, and other generally available company information.

The information compromised from the third party system **does not** contain social security numbers, bank account numbers, passwords, HR data or similar confidential data. Also, ADP's systems were not attacked or compromised.

It has been determined that the stolen email contact information in this system is being used to directly contact clients and others with the "from" address spoofed to look like a valid ADP email address. Please note these emails are not being sent by ADP. These fictitious emails began Thursday September 13, 2007. The emails and their attachments are malicious and are believed to have been sent with the intent to compromise the computer of the email recipient.

Do not open, forward, launch or respond to the email. Immediately delete the email(s) and attachments.

Identify the fraudulent email

- The "from:" address in these emails may have been spoofed to look like it is coming from ADP such as "emplservices292823@adp.com" or "adpcomplaintcenter@adp.com".
- The subject line may read: "Agreement Update for [Your Company Name (Case id: _____)]" or "Complaint Update for [Company Name (Case id. #)]".
- The email may have an attachment named either *Agreement.rtf* or *Agree.rtf* or may instruct you to "download a copy of your complaint."
- The emails may be written in English.

These attacks are sophisticated and you may receive other fraudulent emails. Please be careful not to open any suspicious attachments or to download any files.

The "From" address on the e-mails ADP is using to inform its clients and others about this issue: international@europe.adp.com or your usual contact at ADP.

ADP is in the process of notifying all clients and other parties whose email addresses were maintained in this system and is working with law enforcement and outside forensic experts.

If you are an ADP client and wish to have more information, please contact your local ADP Service Team.

