Last Updated: 9/19/2007 4:00 pm

**What happened?**

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 e-mails 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.

**What is phishing?**

For a good understanding of "phishing," click on the following links: http://www.antiphishing.org/ and http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm.

**What is ADP doing about it?**

ADP has notified all clients and other parties whose email addresses were maintained in this system and may have received the fraudulent emails. The notification instructed them not to open, but to immediately delete, the emails and attachments.

ADP is working with law enforcement and outside forensic experts.

**Is my data secure?**

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.

**How can I 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."

- 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.

**What do I do if I receive the email?**

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

**How do I know my computer is infected?**

If you opened the fraudulent email and also opened one of the following attachments:

- “Agree.rtf” or “Agreement.rtf”

or clicked on a link such as:

- “http://money.chickcat.com/newpdf.php?Evergreen FS, Inc..pdf”
- “http://www.thenervous.com/blog2/images/uploads...Associates.pdf”

Then you should assume your computer is infected.

Symptoms of this issue may include:

- Your computer may appear to have crashed or hung after restart.
- All desktop icons may be missing after reboot of the computer.
- The root of the C drive (C:\) contains the file “microsoft.exe”

**What should I do if my computer is infected?**

- Contact your IT department immediately.
- Disconnect any potentially infected computer immediately from the Internet until the computer has been cleansed.
- From an uninfected computer, search your anti-virus protection provider (e.g., McAfee, Symantec, etc.) for recent information on the following files and then follow your provider’s instructions to remove the files.
    - Complaint.scr, Microsoft.exe, Microsoft.dll, Win32.exe, Win641.exe, and Newpdf.php
- If your computer is infected, immediately take appropriate precautions since your information was likely compromised.
- **As soon as you become aware that your computer has been infected, please contact ADP. If you are an ADP client, please contact your local ADP Service Team. If you have received the fraudulent email and you are not an ADP client, please call 866-623-5661.**

**Who To Contact For Further Technical Assistance?**

If you are an ADP client. please contact your local ADP Service Team.   If you have received the fraudulent email and you are not an ADP client, you may call 866-623-5661 for any further updates.