keypoint

FATCA NEWSLETTER

Issue No. 1189/IT - December 2015

INCREASING INCIDENTS OF "PHISHING" ATTACKS TO GATHER FATCA INFORMATION FROM BANKS

BEWARE OF "PHISHING" ATTACKS FOR US PERSON DATA

We have come across increasing incidents of "phishing" attacks launched by fraudsters targeting financial institutions requiring them to declare information about US persons or their FATCA status. The fraudsters send emails masquerading as "IRS" or "US authorities" requiring financial institutions or individuals to share personal information about US Persons or other FATCA related information through email or FAX. ***Fraudsters have also created a falsely designed W-8BEN form which asks for account information from users. (Please find attached a copy of the false W-8BEN).***

Please note neither IRS nor the local competent authorities require Financial Institutions to disclose information about customers for FATCA purposes other than through the FATCA reporting framework. Moreover, IRS does not require US tax forms like Form W-9, Form W-8BEN or Form W-8BEN-E to be shared with them. These are to be maintained with the Financial Institutions and not to be sent to IRS.

In case you receive any such emails or fax, please verify the validity of such communications and if appropriate report such emails to IRS or the local competent authorities.

A TEXT OF ONE SUCH EMAIL SENT BY FRAUDSTERS IS AS FOLLOWS:

Department of Treasury Internal Revenue Service.

www.irs.gov

Application for a not ordinary resident (non-resident) saver to receive interest without tax taken off or deducted.

ATTN ;

Our records indicate that you are a non-resident alien. As a result, you are exempted from United States of America Tax reporting and withholdings, on interest paid you on your account and other financial dealing to protect your exemption from tax on your account and other financial benefit in rectifying your exemption status.

Therefore, you are to authenticate the following by completing **W-8BEN FORM**, and return to us as soon as possible via fax number enclosed on **W-8BEN FORM**.

If you are a USA Citizen and resident, this **W-8BEN FORM** is not meant for you, please indicate "USA Citizen/Resident" on the form and return it to us. We shall then send you a form W9095.

When completing **W-8BEN FORM**, please follow the steps below

1. We need you to provide your permanent address if different from the current mailing address on your **W-8BEN FORM**, you must indicate if a non-USA resident, your country of origin to support your non-resident status (if your bank account or other financial dealing has a USA address for mailing purpose).

2. If any joint account holder are now USA residents or Citizen, or in any way subject to USA tax reporting laws, Please check the box in this section.

3. Please have all account holders sign and date the form separately and fax it to the above-mentioned number.

Please, complete **W-8BEN FORM** attached" and return to us within 1 (one) week from the receipt of this letter by faxing it, to enable us update your records immediately if your account or any other financial benefits are not rectified in a timely manner, it will be subject to USA tax reporting and back up withholding (if back up withholding applies, we are required to withhold 30% of the interest paid to you).

What you need to do
Print out the attached notification and complete the attached **W-8BEN FORM** and Fax same along with a copy of your international passport to fax number on the form within 7 working days.

List of required documents:

1. A copy of filled **W-8BEN FORM**.

2. A photocopy of the photo page of your international passport.

Keep this notice for your records. If you need assistance, please do not hesitate to contact us. If you should receive multiple notifications, it means previous filled form was not properly filled and as such, we need you to refill needed column and re-fax to us

WHAT IS PHISHING?

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords, bank account details and credit card numbers, online.

Types of Phishing

1. **Spear Phishing** – Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.

2. **Clone Phishing** – A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original.

3. **Whaling** – Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks. In the case of whaling, the masquerading web page/email will take a more serious executive-level form. The content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email is often written as a legal subpoena, customer complaint, or executive issue.

IRS NOTIFICATION RELATED TO "PHISHING" AND OTHER "ELECTRONIC" FRAUDS

IR-2015-129, Nov. 19, 2015

WASHINGTON — The Internal Revenue Service, state tax administrators and the private-sector tax industry today announced a new campaign aimed at encouraging more people to protect their personal and financial data online and at home.

It is clear that increasingly sophisticated identity thieves have access to excessive amounts of personal and financial data, which they buy and sell on the black market, and use this data to file fraudulent tax returns using victims' names and Social Security numbers. While the IRS, states and tax industry are taking new steps to toughen their systems to protect taxpayers, there are also things people can do as well.

The IRS, states and tax industry are urging the public to take active steps to protect themselves. The partners are encouraging people to:

- **Use security software to protect computers** – This includes a firewall and anti-virus protection. If tax returns or sensitive data are stored on the computers, encrypt the files. Use strong passwords.

- **Beware of phishing emails and phone scams**– A common way for identity thieves to steal names and Social Security numbers, passwords, credit card numbers, bank account information is to simply ask for it. Clever criminals pose as trusted organizations that you recognize and send spam emails, calls or texts. Their email may ask you to update a bank account or tax software account and provide a link that to a fake website that is designed solely to steal your logon information.

They may call posing as the IRS threatening you with jail or lawsuits unless you make an immediate payment. They may provide an attachment which, if you download, will infect your machine and enable the thief to access sensitive files or track your key strokes.

- **Protect personal information**– Do not routinely carry your Social Security number. Properly dispose of old tax returns and other sensitive documents by shredding before trashing. Check your credit reports and Social Security Administration accounts at least annually to ensure no one is using your good credit or using your SSN for employment. Oversharing on social media also gives identity thieves even more personal details.

(Source – IRS Newsletter ***IR-2015-129***, *Nov. 19, 2015*)

Persons who suspect they are the subject of a "phishing" scam should report the matter to the Treasury Inspector General for Tax Administration (TIGTA) at 800-366-4484, or through TIGTA's secure website. Any suspicious emails that contain attachments or links in the message should not be opened, and the email should be forwarded to phishing@irs.gov.

(Source – IRS Newsletter ***IR-2014-92***, *Sept. 24, 2014*)

For more information, enquiries and events please do not hesitate to contact: *Ranjith Kumar* on ranjith.kumar@keypoint.me or *Chahira Ashcroft* on chahira.ashcroft@keypoint.me