

IRS Issues Fraud Alert to Financial Institutions Complying with Foreign Account Tax Compliance Act (FATCA)

Thursday, September 25, 2014

The **Internal Revenue Service** issued a [fraud alert](#) for international financial institutions complying with the **Foreign Account Tax Compliance Act (FATCA)**. According to the report, scam artists posing as the IRS – through attacks known as “phishing attacks” – have fraudulently solicited financial institutions seeking account holder identity and financial account information. Financial institutions [regularly face these threats](#), but all organizations can be subjected to them and need to have safeguards in place.

Of course, phishing attacks can come in many different forms. For example, emails that impersonate a bank ask customers to click a link that directs them to a phony website made to look like the bank’s site, but which is operated by the attackers and prompts the customers to disclose confidential information. There are some steps an organization can take to address this risk:

- [Know your systems and your IT department.](#) Management needs to work closely with IT and other departments to identify all of the company’s sites and systems at risk. Management also needs to assess whether its IT department has the appropriate resources to address these risks – resources could include more experienced individuals and more sophisticated software and other tools.
- [Help your employees learn how to recognize a phishing attack and respond.](#) Some employees may still think “phishing” is something you do with a worm and a hook. Companies would be wise to inform employees about these dangers and help them to recognize attacks at work and at home. This is particularly the case as more employees telecommute or otherwise work remotely. Employees also should be instructed on how to report an incident that could be an attack.
- [Have a response plan.](#) When these kinds of attacks occur, they will require prompt action by persons ready and able to act. In developing a plan, consider the following questions. Who in the company will be altered of the attack? Is your list complete and include appropriate persons from management, IT, legal, risk management, compliance, customer/employee relations, and other relevant departments? Does the list have up to date emergency contact information? What external vendors need to be alerted? Do you have a communications strategy to inform employees, customers, clients, government agencies? How should you communicate the plan internally, and how often? Have you tested the plan?

In the case of the IRS alert, it reminds these institutions that the IRS does not require financial institutions to provide specific account holder identity information or financial account information over the phone or by fax or email. Further, the IRS does not solicit FATCA registration passwords or similar confidential account access information. The alert also provides financial institutions and their representatives with information on how they should report incidents.



Article By [Jackson Lewis P.C.](#)
[Joseph J. Lazzarotti](#)
[Workplace Privacy Blog](#)

[Criminal Law / Business Crimes](#)
[Consumer Protection](#)
[Tax](#)
[Financial Institutions & Banking](#)
[Communications, Media & Internet](#)
[Labor & Employment](#)
[Administrative & Regulatory](#)
[All Federal](#)

Source URL: <https://www.natlawreview.com/article/irs-issues-fraud-alert-to-financial-institutions-complying-foreign-account-tax-compl>