

**F. No. 500/62/2015-FTTR-III
Government of India
Ministry of Finance
Department of Revenue
Central Board of Direct Taxes
(Foreign Tax & Tax Research Division)**

Date: 6th January, 2021

To

All Pr. CCsIT/ Pr. DGsIT/ CCsIT/ DGsIT

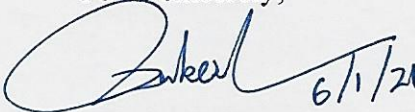
Sir/Madam,

Subject: Protocol for handling breach of information exchanged under the tax treaties– reg

Maintaining confidentiality of data is one of the cornerstones of our tax administration. This assumes special significance when information exchanged under the provisions of tax treaties is involved. Recently, vide CISO Instruction No. 2 dated 27th November, 2020, the Income Tax Department (ITD) Information Security Policy and the ITD Acceptable Usage Policy was issued.

2. A protocol for handling breach of information exchanged under the tax treaties (Breach Protocol) has been prepared as per international standards and has been approved by the Information Security Committee (ISC). This Breach Protocol is hereby circulated for adoption by all offices under your charge that are involved in handling of treaty exchanged information.

Yours sincerely,



(Rakesh Gupta)

Chief Information Security Officer, CBDT &
CIT (C&S), CBDT

Encl.: Breach Protocol Document

INCOME TAX DEPARTMENT PROTOCOL ON BREACH OF TREATY EXCHANGED DATA

1. Introduction

1.1 This document is meant to elucidate the Breach Protocol which would be activated as a special case of Incident Management as a part of the ITD Information Security Policy 2020. In this protocol a breach refers to an incident of inappropriate access, disclosure or use of confidential information or a failure of data safeguards. This protocol would get activated when it is discovered that there has been a security breach involving treaty exchanged information.

1.2 The key elements that are covered in this document are:

- Governance of a breach
- Breach Management
- Communication Protocol

2. Governance of a breach

2.1 *Before breach protocol is triggered*

Before a breach is announced, there has to be sufficient evidence for declaration of a breach and the consequent activation of the breach protocol. The breach protocol is to be activated by the Information Security Committee (ISC) based on inputs from the concerned Local Information Security Committee (LISC) under whose jurisdiction the breach is supposed to have occurred. In case the intimation is received by the ISC other than through a report of the LISC, the ISC may choose to call an immediate report from the LISC before activating the breach protocol.

2.2 Once the ISC is convinced that the security incident warrants the activation of breach protocol due to the seriousness of the matter involving treaty exchanged information, the breach protocol gets activated. The steps involved in the breach protocol would be discussed in the next section on Breach Management.

2.3 The entire breach protocol would be governed by the ISC and all the stakeholders would have to report on the progress of the breach management to the ISC.

3. Breach Management

3.1 The first action under the breach protocol will be for key stakeholders and decision-makers to meet. The ISC will convene a meeting involving all the stakeholders in order to ascertain the facts and finalise further course of action.

3.2 *Identification*

The ISC will designate the concerned Local Information Security Committee as the breach management task force which will involve all relevant stakeholders and will report directly to the ISC.

3.3 If the breach is due to internal sources, the task force would immediately move towards eradicating the cause of the breach and taking necessary remedial action. However, if the breach involved external agents such a hack from an external source, all susceptible communication links should be immediately suspended till security is reestablished and adequately tested. The ISC and the task force would need to ensure that adequate resources are deployed in order to resolve the matter on top priority.

3.4 The various steps of the Breach Management are explained as below:

Containment

3.4.1 The damage being done by those responsible for the security incident should be contained, for example, by stopping a cyber-incident from spreading to other networks and devices both within the organisation and beyond. Containment typically comprises a number of concurrent actions aimed at reducing the

immediate impact of the breach, primarily by removing the attacker's access to systems. The objective of containment is not always to return (directly) to a functional state as usual, but to make best efforts to return to functionality as normal, prevent further disclosure of information and mitigate the risk of damage to individuals affected, while continuing to analyse the incident and plan longer-term remediation.

3.4.2 Creating separate containment strategies for different types of major-cyber security attacks should be considered, with clear criteria to facilitate decision-making. These criteria can include evaluating the:

- Damage to operations or assets, including availability of services;
- Need for evidence preservation (see Phase 4 below);
- Time and resources needed to implement the strategy;
- Effectiveness of the strategy (e.g. partial containment, full containment); and
- Duration of the solution (e.g. emergency work-around to be removed in a few hours, temporary work-around to be removed in a few weeks, or a permanent solution).

3.4.3 Based on the type and extent of breach as above, the task force created by the ISC would formulate a containment strategy.

Eradication

3.4.4 After an incident has been contained, eradication is often required to eliminate key components of the incident (for example, removing the attack from the network and disabling breached user accounts), as well as identifying and mitigating vulnerabilities that were exploited. During the eradication process of a cyber-incident in particular, there are a number of actions that can be taken, which include:

- Identifying all affected hosts;
- Carrying out malware analysis;
- Checking for further responses from the attacker;
- Developing a response if the attacker uses a different method of attack; and
- Allowing sufficient time to ensure that the network is secure and that there is no response from the attacker.

3.4.5 Effective eradication plans must be executed with speed and precision because cyber-attackers often create "back doors" which would enable them to continue to operate once they sense that they have been discovered and that eradication is underway. There are many steps that attackers take to either continue the attack during eradication or avoid identification, all of which need to be anticipated.

3.4.6 The task force would take necessary steps for eradication of the threat once it has been contained.

Remedial Action

3.4.7 The task force would suggest necessary steps to ensure that adequate security measures are instituted so as to prevent security incidents of similar nature to recur.

3.4.8 Such suggestions would be considered by the ISC and thereafter adopted across the Department as supplementary to the Information Security Policy of the Department.

4. Communication Protocol

4.1 *Domestic regulatory communication requirements*- The ISC would intimate all domestic stakeholders of the breach as required under the extant domestic laws within 48 hours of the breach coming to the knowledge of the ISC.

4.2 *Communicating to the providers of breached data*- Breached data within the ambit of the breach protocol would have been received from foreign Competent Authorities. The concerned FT&TR Division of CBDT would intimate the foreign Competent Authority of the breach within 48 hours of the breach incident coming to the knowledge of the ISC. After the first notification, continued communication with the concerned exchange partner(s) will be necessary, to inform them of any relevant developments as more detailed information becomes available as a result of the breach investigation, and specifically where the exchange partner may be required to take action, e.g. to notify impacted persons as they are identified. The flow of communications with exchange partners should follow a plan ideally developed at the outset of the occurrence of a breach of data, and should be based on the particular characteristics of the breach. Notification of exchange partners and subsequent communications would generally be done by electronic or physical mail to the address of the partner Competent Authority, with supporting telephone discussions as necessary. The communication of taxpayer information, if necessary, should be channelled through means appropriate to the sensitivity of the information transmitted.

Early notifications would generally be expected to address the following points:

- Where the breach occurred (e.g. which organisation, which division or system of a tax administration);
- The type of breach (e.g. cyber-attack, data theft by an insider, lost documents or storage media);
- The type of data involved (e.g. EOI on request file, CRS data, CbC data);
- Exchange partner jurisdictions impacted (or expected to be impacted);
- Actions being taken to contain, eradicate and analyse the situation; and
- Central point of contact and/or other contact points.

As the nature and facts surrounding a breach become clearer and containment and eradication measures move forward, it will generally be appropriate to update exchange partners. Further updates would generally be expected to address the following points:

- Whether the containment and eradication actions have been effective in addressing the underlying causes of the breach;
- Whether it is considered that exchanges of information may therefore resume;
- What remediation, recovery and adjustment measures will be adopted to prevent similar breaches from happening in the future, including long term measures or projects; and
- What remedial actions were taken or sanctions were imposed as a consequence of the breach.

4.3 *Communicating with the Co-ordinating Body Secretariat*- As per the international requirement International agreements on the automatic exchange of information (AEOI) generally include requirements for Competent Authorities to immediately notify each other regarding breaches and sanctions consequently imposed or remedial actions taken. Therefore, the concerned Competent Authority, i.e., Joint Secretary of FT&TR Division must notify the Co-ordinating Body Secretariat within 48 hours of the incident. The contents of the communication would include details as indicated in paragraph 4.2 above.

4.4 *Communicating with other Competent Authorities for temporary suspension of exchanges* – In consonance with the Global Forum plan for breaches, the other Competent Authorities may be informed through the Co-ordinating Body Secretariat or the CTS Secretariat to temporarily suspend sending information to India till the issue is resolved.

4.5 *Communicating to affected persons or taxpayers* - A data breach will also affect the persons whose data has been breached, and may have serious implications for them such as vulnerability to financial fraud. Therefore, the concerned taxpayer would also have to be informed through the Investigation Division of CBDT within 48 hours of the breach coming to the knowledge of the ISC.

4.6 *Communicating within the tax administration* - The breach incident would also need to be brought to the knowledge of the ITD depending upon the seriousness of the incident so as to alert the field authorities.

4.7 *Communicating to the public* – Depending upon the nature of breach, the ISC may consider issuing appropriate public and/or external communications (e.g. website statements, or targeted messages) to address different domestic stakeholders’ questions and concerns.

4.8 *Subsequent Updates* – The foreign Competent Authorities and international bodies have to be updated periodically about the progress in breach management.
