

EDPB
National DPAs (via EDPB Secretariat)
Brussels

Africa House
70 Kingsway
London WC2B 6AH
DX 37954 Kingsway
T: +44 20 3321 7000
www.mishcon.com

Cc: PETI, EU FATCA Petitioners

2 January 2025

London | Cambridge | Oxford | Hong Kong | Singapore

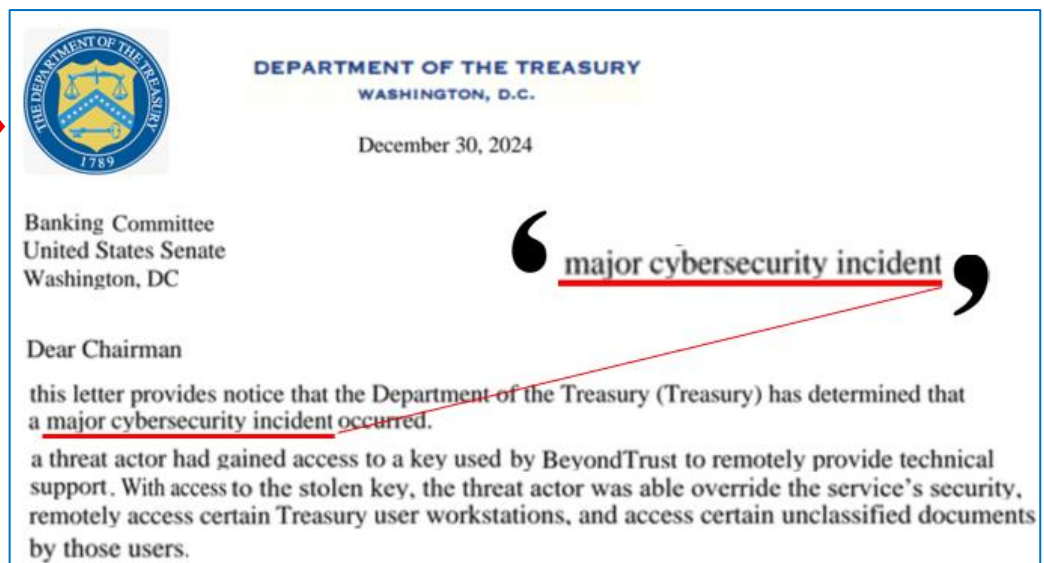
FATCA | US Treasury hacking shows urgency of upholding GDPR principles

US Treasury hacked

On 30 December 2024, the US Treasury sent a [letter to the US Senate](#) confirming that state-backed hackers (reportedly from China) were able to roam free in its systems following the theft of a remote access key used to provide technical assistance to Treasury office workers.



"Major incident"



(again, and again)

This is not the first time that the US Treasury got hacked. On 13 December 2020, the White House acknowledged reports of a [cyberattack on the US Treasury](#) by another foreign government (reportedly, Russia).



What about FATCA data?

The latest hacking enabled criminals to take remote control of desktops. Whilst the US Treasury sought to reassure that 'no classified information' was accessed, it could have affected FATCA data, as our research shows that the affected tool (a remote access system called [BeyondTrust](#)) is [used by the IRS](#) (see also [here](#)), as well as 20,000 other customers, including 75% of the Fortune 500, across 100+ countries. As FATCA does not require any indicia of wrongdoing, the latest incident shows that FATCA exposes millions of compliant citizens to unnecessary data protection and data security risks.



Shrugging from EU Commission, and EDPB "awol"



At the time of the previous cyberattack, the European Commission refused to answer an [MEP's written question](#) about the implications for FATCA, limiting itself to [state](#) that FATCA was a matter for national data protection authorities, thus perpetuating the endless game of 'ping-pong', 'forbearance and institutional deference' designed to frustrate any attempt to enforce the GDPR in this area, which is recognised as a "long-standing issue". The EDPB is directly responsible for this situation, aware as it is of the [inconsistent application](#) of the GDPR by EU Member States in this area and [consistently refusing](#) to engage its powers under Art. 70 GDPR, leaving [courageous](#) national data protection authorities to fend for themselves, without any support from a body that was created to guarantee a higher level of data protection in the EU (supposedly). The whole thing looks like a sad game of snakes and ladders. It is only to be hoped that this latest incident will convince the EDPB to make a statement on the application of its [Guidelines 02/2024 on international data transfers](#) to FATCA.