Client Alert | White Collar/Investigations

Criminal consequences of the use of leaked data by tax authorities

September 2016

Authors: Jonathan Pickworth, Joseph Carroll, Jonah Anderson, Deborah Williams

Leaks of confidential information are becoming more common. Businesses and individuals may face scrutiny by investigative agencies following leaks of information from third parties or by employees. Businesses in particular face risks regarding potential tax investigations, especially given the proposed new offence of failing to prevent tax evasion.

Earlier this month, it was widely reported that the Danish government plans to purchase data from the 'Panama Papers' leak in order to investigate whether hundreds of Danish citizens who feature in the data may have evaded tax.

The Danish transaction is the latest example of a relatively recent development in the fight against tax evasion. Over the last decade, tax authorities in a number of countries (including the UK) have, in pursuit of unpaid tax, acquired large quantities of electronic data that were obtained from businesses without authorisation or, in some cases, unlawfully.

The willingness of tax authorities to use leaked data in their investigations presents a particularly serious risk to businesses that are affected by such leaks, in light of the proposed 'failure to prevent' offence regarding tax evasion.

Corporate criminal liability and the expansion of the 'failure to prevent' approach

At present, under English law, unless expressly stated otherwise a company will only be criminally liable where the necessary mental element of an offence is attributable to one or more persons (such as the CEO or members of the board) who at the relevant time represented the company's 'directing mind'. This is often very difficult to prove in practice.

The Bribery Act 2010 addressed this difficulty by creating an offence of failure to prevent bribery[1], which requires only that a person associated with the company (such as an employee or an agent) has engaged in bribery to obtain or retain business (or an advantage in the conduct of business) for the company. The company has a defence if it can show that it had in place adequate procedures designed to prevent such conduct. This new approach has incentivised corporate anti-corruption efforts, prompting companies to review their anti-corruption measures and ensure that they are sufficiently robust to (if necessary) provide a defence.

The government intends to expand the 'failure to prevent' approach to tax evasion and subsequently to other economic crimes, taking the Bribery Act offence as a guide. In July this year, a consultation closed on the creation of an offence that would criminalise a company's failure to prevent associated persons facilitating tax evasion, in much the same way as the Bribery Act offence (and with a similar defence relating to 'reasonable prevention procedures'). It is also proposed that deferred prosecution agreements be available in relation to

[1] Section 7 of the Bribery Act 2010.

the new offence, as with the Bribery Act offence. In a speech earlier this month, the Attorney General Jeremy Wright confirmed that, in addition to the planned tax evasion offence, the government will soon consult on plans to extend the scope of the 'failure to prevent' approach to other economic crimes, such as money laundering, false accounting and fraud.

The new tax offence will have significant implications for all businesses, especially those in the banking and professional services sectors (as discussed in a previous alert), but should be of particular concern to businesses whose data is leaked or stolen or who are affected by the leak of data from a third party. Tax authorities have demonstrated that they are willing to pay to acquire such data and that they will share it with others. Foreign tax authorities have previously shared leaked or stolen data with HMRC, and HMRC has had discussions with other UK investigative agencies about sharing such data in order to facilitate the investigation of other economic crimes.

At present, the 'directing mind' doctrine makes it difficult for a business to be prosecuted for such crimes. Once the new 'failure to prevent' offences become available, a business that is affected by a leak from which HMRC acquires data is likely to face a significantly higher risk of prosecution.

HMRC's approach to leaked or stolen information

While prosecutions for tax-related offences increase year on year, HMRC has historically preferred to address potential tax fraud identified via leaked information on a civil basis. HMRC is a revenue-gathering body; litigation carries risk and cost, and in complex criminal tax evasion cases the disclosure regime has proved to be challenging for HMRC and the Crown Prosecution Service. When dealing with a large class of tax evaders, a civil fraud inquiry reduces investigation costs for HMRC, shifts the burden to the recalcitrant taxpayer and is more likely to lead to a favourable financial outcome. A civil fraud inquiry also allows HMRC to avoid the risk that a criminal defendant will raise legal arguments relating to the admissibility of evidence obtained from stolen information.[2]

A business under investigation regarding the tax evasion offence may first seek to argue (if possible) that no tax evasion took place, then – if that argument is unsuccessful – rely on the adequacy of its compliance measures. Deferred prosecution agreements are expected to be available in relation to the new tax evasion offence, but it is unclear whether an argument that no tax evasion took place would be compatible with any degree of cooperation required to obtain a deferred prosecution agreement.

Conclusion

The acquisition of stolen information by tax authorities could be seen as validating the underlying criminal conduct and, if data is purchased, as spending taxpayers' money to reward (and thus incentivise) criminal activity. Tax authorities appear to take the view that the leaker's conduct, while unlawful, serves society's interests insofar as the data can be used to pursue revenue collection and combat criminal activity on a larger scale.

Regardless of one's view on whether the tax authorities' ends justify their means, large-scale data leaks can be expected to continue – see for example last week's publication of data leaked from the Bahamian corporate registry. In the UK, absent a change in government policy or a court decision, businesses affected by such leaks can expect to be increasingly exposed to investigation and criminal prosecution for 'failure to prevent' offences. Before these offences are implemented, businesses should ensure that their compliance measures are sufficiently robust to provide a defence.

[2] For example, under section 78 of the Police and Criminal Evidence Act 1984.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000