Ben Verwaayen reappointed as a Board Member at Ofcom

Ben Verwaayen, former CEO of BT plc and Alcatel-Lucent is presently General Partner at Keen Venture Partners, an investor in high tech scale ups. Ben is also a non executive director at Akamai in Boston US and AkzoNobel in Amsterdam.

This role is remunerated at £42 519 per annum. This reappointment has been made in accordance with the Cabinet Office's Governance Code on Public Appointments. The process is regulated by the Commissioner for Public Appointments.

The Government's Governance Code requires that any significant political activity undertaken by an appointee in the last five years is declared. This is defined as including holding office, public speaking, making a recordable donation or candidature for election. Ben has made no such declarations.

Property and cleaning companies wound-up for abusing credit agreements

Swanholme Limited and Nistor International Limited were both wound up in the public interest in the High Court on 24 September 2019. The Official Receiver has now been appointed as the Liquidator.

In considering the petition to wind up the company, the court heard that Swanholme was incorporated in November 2015, advertising itself online as a company that specialised in short-term full-serviced rental accommodations in prime locations throughout Europe.

Following complaints, however, the Insolvency Service conducted confidential investigations into the Swanholme and found several incidents of misconduct.

Swanholme filed false and misleading accounts at Companies House. This information was trusted by at least one creditor when it provided foreign hotel and car rental services to the company on a bill-back basis in the region of £8,000-9,000. Swanholme, however, failed to pay the creditor back.

For three months Swanholme traded saying they were registered to an address in Leatherhead but did not reveal to creditors that their tenancy agreement had been terminated due to non-payment of fees.

And the company failed to produce its books to investigators and this has

meant the Insolvency Service has been unable to establish the true level of debt held by Swanholme.

During the same hearing, the court also considered a connected company, Nistor International Limited, which had assisted Swanholme in obtaining credit.

Nistor International was incorporated in May 2018 and advertised itself as company that provided cleaning services for nuclear environments and the government.

The court heard that Swanholme presented Nistor International as a reference in support of at least one credit application and requested that fuel cards for Swanholme be delivered to Nistor International's registered office in Hove, East Sussex.

Additionally, several payments were made between Swanholme Limited and Nistor International Limited by way of a pre-paid credit card but as neither company has co-operated with the enquiries, investigators have not been able to determine the nature of the relationship between the two companies.

In court, Judge Briggs stated that the misleading financial accounts lodged with Companies House presented a "real prejudice to the lenders and public", while praising the diligence of the Insolvency Service investigator.

David Hill, Chief Investigator for the Insolvency Service, said

> The systematic abuse of creditors to gain funds enabled the company directors behind Swanholme and Nistor International to benefit at the expense of legitimate businesses.

> There should be no doubt that whenever we discover there are serious failings by companies and their business dealings, as there were with these companies, that we will investigate and take action to close down their activities.

By virtue of the winding up order all public enquiries concerning the affairs of the companies should be made to: The Official Receiver, Public Interest Unit , 4 Abbey Orchard Street, London, SW1P 2HT. Telephone: 0207 637 1110 Email: piu.or@insolvency.gov.uk.

Swanholme Limited (company registration number 09887876) was incorporated on 25 November 2015. The company's registered office is at: PO Box 4385, 09887876: COMPANIES HOUSE DEFAULT ADDRESS, Cardiff, CF14 8LH

Nistor International Limited (company registration number 11357073) was incorporated on 11 May 2018. The company's registered office is at: Gemini House, 136-140 Old Shoreham Road, Hove, England, BN3 7BD

The petitions were presented under s124A of the Insolvency Act 1986 on 15 August 2019 at the High Court of Justice.

The Official Receiver was appointed as liquidator of the companies on 24 September 2019 by Chief ICCJ Briggs, a Judge of the High Court of Justice, Business and Property Courts of England and Wales.

Company Investigations, part of the Insolvency Service, uses powers under the Companies Act 1985 to conduct confidential fact-finding investigations into the activities of live limited companies in the UK on behalf of the Secretary of State for Business, Energy & Industrial Strategy (BEIS). Information about how to complain about a live company.

Information about the work of the Insolvency Service.

You can also follow the Insolvency Service on:

UK and US sign landmark Data Access Agreement

The world-first UK-US Bilateral Data Access Agreement will dramatically speed up investigations and prosecutions by enabling law enforcement, with appropriate authorisation, to go directly to the tech companies to access data, rather than through governments, which can take years.

The Agreement was signed with US Attorney General William P. Barr in Washington DC, where the Home Secretary also met security partners to discuss the two countries' ever deeper cooperation and global leadership on security.

Home Secretary Priti Patel said:

> Terrorists and paedophiles continue to exploit the internet to spread their messages of hate, plan attacks on our citizens and target the most vulnerable.
>
> As Home Secretary I am determined to do everything in my power to stop them. This historic Agreement will dramatically speed up investigations, allowing our law enforcement agencies to protect the public.
>
> This is just one example of the enduring security partnership we have with the US and I look forward to continuing to work with them and global partners to tackle these heinous crimes.

US Attorney General William P. Barr said:

> This Agreement will enhance the ability of the United States and the United Kingdom to fight serious crime – including terrorism, transnational organized crime, and child exploitation – by allowing more efficient and effective access to data needed for quick-moving investigations.
>
> Only by addressing the problem of timely access to electronic evidence of crime committed in one country that is stored in another, can we hope to keep pace with twenty-first century threats.
>
> This Agreement will make the citizens of both countries safer, while at the same time assuring robust protections for privacy and civil liberties.

The current process, which see requests for communications data from law enforcement agencies submitted and approved by central governments via Mutual Legal Assistance (MLA), can often take anywhere from six months to two years. Once in place, the Agreement will see the process reduced to a matter of weeks or even days.

The Agreement will each year accelerate dozens of complex investigations into suspected terrorists and paedophiles, such as Matthew Falder who was sentenced in 2018 of 137 offences after an eight-year campaign of online child sexual abuse, blackmail, forced labour and sharing of indecent images. His case highlights the need to speed up these investigations.

The US will have reciprocal access, under a US court order, to data from UK communication service providers. The UK has obtained assurances which are in line with the Government's continued opposition to the death penalty in all circumstances.

Any request for data must be made under an authorisation in accordance with the legislation of the country making the request and will be subject to independent oversight or review by a court, judge, magistrate or other independent authority.

The Agreement does not change anything about the way companies can use encryption and does not stop companies from encrypting data.

It gives effect to the Crime (Overseas Production Orders) Act 2019, which received Royal Assent in February this year and was facilitated by the CLOUD Act in America, passed last year.

Open letter to Facebook Chief Executive Mark Zuckerberg

The Home Secretary has also published an open letter to Facebook, co-signed with US Attorney General William P. Barr, Acting US Homeland Security Secretary Kevin McAleenan and Australia's Minister for Home Affairs Peter Dutton, outlining serious concerns with the company's plans to implement end-to-end encryption across its messaging services.

Addressed to Facebook's CEO, Mark Zuckerberg, the letter calls for a halt to the proposals unless the company can provide assurances that there will be no reduction in Facebook's ability to keep its users safe and enable law enforcement access to content in exceptional circumstances in order to protect the public.

This issue is not just about one company. However, the letter makes clear particular concerns with Facebook's plans and the impact they would have on efforts to tackle online child sexual abuse and terrorism.

Facebook's proposals would put its own vital work keeping people safe at risk. In 2018, Facebook made 16.8 million reports of child sexual exploitation and abuse content to the US National Center for Missing & Exploited Children (NCMEC), 12 million of which it is estimated would be lost if the company pursues its plan to implement end-to-end encryption. The National Crime Agency estimates that these referrals from Facebook have led to more than 2,500 arrests in 2018 and almost 3,000 children safeguarded.

The Government is clear in its commitment to the right to privacy and does not, however, believe the requirement to provide exceptional access to data where a warrant is in place, undermines this in any way. Law enforcement and other agencies must, in certain circumstances, be able to access data, with strong and independent authorisation and oversight.

The Home Secretary added:

> Tech companies like Facebook have a responsibility to balance privacy with the safety of the public.
>
> So far nothing we have seen from Facebook reassures me that their plans for end-to-end encryption will not act as barrier to the identification and pursuit of criminals operating on their platforms.
>
> Companies cannot operate with impunity where lives and the safety of our children is at stake, and if Mr Zuckerberg really has a credible plan to protect Facebook's more than two billion users it's time he let us know what it is.

Letter from the Home Secretary and others to the CEO of Facebook

The letter, signed by Home Secretary Priti Patel, US Attorney General William P. Barr, US Secretary of Homeland Security (Acting) Kevin K. McAleenan and

Australian Minister for Home Affairs Peter Dutton, concerns Facebook’s ‘Privacy First’ proposals.

Open letter to Mark Zuckerberg

This open letter to Mark Zuckerberg is from the Home Secretary, alongside US Attorney General Barr, Secretary of Homeland Security (Acting) McAleenan, and Australian Minister for Home Affairs Dutton.

The letter requests that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for law enforcement to obtain lawful access to the content of communications.