Teletext to pay back over £7 million for all outstanding refunds

The Competition and Markets Authority (CMA) opened an investigation into Teletext Holidays and its sister travel operator, Alpharooms.com (Alpharooms), on 4 February after receiving hundreds of complaints. This showed that people were not receiving refunds they were owed within 14 days, as required by law, for package holidays cancelled by the company due to the pandemic.

On 30 April, the CMA informed Truly Holdings Ltd, the company that operates Teletext Holidays and Alpharooms, that it was preparing to take court action against the firm for over £7 million in outstanding refunds owed to its customers.

Truly Holdings Ltd has now signed formal commitments, known as undertakings, that ensure affected customers still owed a refund will get their money back. This includes a repayment schedule that prioritises refunds to customers with the longest-standing claims.

Andrea Coscelli, Chief Executive of the CMA, said:

> There’s no excuse for travel firms to delay refunding customers what they are legally owed, even in these extraordinary times. Companies should be doing the right thing without the threat of court action.
>
> As a result of our work, customers who have waited many months for their money back from Teletext Holidays and Alpharooms will now receive a full refund.
>
> With international travel resuming and many people considering long awaited trips abroad, all package holiday firms must give refunds within 14 days where these are due, and should also provide clear cancellation information, so that no one else is unnecessarily put through this ordeal.

Having carefully reviewed Truly Holdings Ltd’s financial information and how quickly it can realistically make the repayments, the CMA has accepted its commitment to pay back all customers owed refunds by 31 August 2021 at the latest. The timeframe that has been agreed balances the challenges experienced by the travel sector as a result of the pandemic with the need to get customers their money back in full as quickly as possible. The company has also committed in its undertakings to refunding in full within 14 days any package holidays it cancels due to the COVID-19 pandemic going forward.

To ensure that the company adheres to its commitments, it has agreed to provide the CMA with regular reports on the progress of its repayments. If

the firm fails to repay customers according to the undertakings, the CMA is prepared to take it to court.

Customers waiting for their money back should visit www.teletextholidays.co.uk or www.alpharooms.com from 28 May, where there will be dedicated pages explaining the process regarding refunds and a webform enabling customers to request a cash refund. In addition, Teletext Holidays and Alpharooms package holiday customers who have not received cash refunds but who have Refund Credit Notes for their cancelled trips, which have not expired or been redeemed, should receive an email from the company shortly, asking them to confirm whether they want a refund.

Today's announcement follows significant action by the CMA in relation to holiday cancellations during the coronavirus (COVID-19) pandemic, including securing refund commitments from LoveHolidays, Lastminute.com, Virgin Holidays, and TUI UK. The CMA has also written to over 100 package holiday firms to remind them of their obligations to comply with consumer protection law, and warned package holiday companies to respect the refund rights of holidaymakers ahead of the summer period.

Further information on this case can be found on the COVID-19 cancellations: package holidays web page.

Notes to editors

1. Teletext Holidays is the trading name of Truly Travel Limited, which is a subsidiary of Truly Holdings Limited. Truly Travel Limited and Alpha Holidays Limited (which trades as Alpharooms.com) are both subsidiaries of Truly Holdings Limited.

2. Truly Holdings Ltd has agreed to a schedule of repayments, where customers who are still owed cash refunds for bookings cancelled due to the COVID-19 pandemic on or before 31 July 2020 will be refunded by 30 June 2021; customers with bookings cancelled between 1 August 2020 and 31 October 2020 will be refunded by 31 July 2021; and customers with bookings cancelled between 1 November 2020 and 24 May 2021 (inclusive) will be refunded by 31 August 2021.

3. The CMA sent a letter before claim to Truly Holdings Limited on 30 April 2021. This outlined that the CMA intended to apply to the court for an order under section 217 of the Enterprise Act 2002 requiring the company to comply with its obligations under the Package Travel and Linked Travel Arrangements Regulations 2018.

4. The CMA's investigation relates to package travel holidays booked with Teletext Holidays and Alpharooms, not flights or accommodation booked on a standalone basis.

5. Where package holidays are cancelled and consumers are entitled to a full refund under the Package Travel Regulations, those refunds must be provided within 14 days of the cancellation.

Commander of Strategic Command RUSI conference speech

Thank you, Secretary of State and let me add my own welcome to our second annual conference. Fifteen months have passed since we gathered at RUSI on Whitehall for the inaugural Strategic Command conference and it has since been a seminal period for Defence, and for Strategic Command in particular. None of us could have imagined what those 15 months had in store. COVID 19 dominated every aspect of our lives, and Defence was no exception. We're going to spend most of today focused on the future, but it would be wrong not to dwell briefly on the pandemic and call out the remarkable work that sometimes goes unsung in Strategic Command.

Defence Digital enabled secure remote working extraordinarily quickly and effectively. Defence Support was central to the procurement of PPE and rapid distribution of vital medical supplies. Defence Intelligence provided critical medical intelligence to the heart of government decision making. And our overseas bases, remote and cut off for sustained periods of time, managed the risk with extraordinary skill and discipline and supported stretched local medical infrastructure. But I want in particular to shine a light on the Defence Medical Services who have been fully mobilised and embedded on the frontline of the NHS for 14 months: consultants, doctors, nurses, combat medics, paramedics, medical support staff and carers. They have done no more or less than their NHS colleagues, but their skills – military and medical – have been vital. They shun the limelight and claim no credit or recognition, but I want to pay tribute to them, to recognise the burden they have borne, the sacrifices they have made, the suffering and grief they have witnessed and to thank them as publicly as I can. I am immensely proud of them all.

The pandemic has been a global tragedy. But from every fight we draw lessons, and the pandemic has been no different. I want to pick out three. First it has highlighted the importance of national resilience and in particular our reliance on cyberspace as a domain – the internet has been a lifeline for many during lockdown. But it has also been a conduit for disinformation – fraying the bonds of society, the seams of alliances and undermining the workings of democracy including our healthcare responses, all fuelled by digital authoritarians.

Just in the last few months cyberspace has been the vector for espionage. From Solarwinds, which was attributed to Russia; the Finnish parliament, attributed to China; the crippling of critical US national infrastructure

through ransomware attacks and, chillingly – on the Irish health service in the midst of the pandemic, both attributed to Russian cyber actors. Now the UK is ranked by the Harvard Kennedy School's Belfer Centre as one of the world's three leading cyber powers. The record investment in the Integrated Review reinforces that.

I want to underscore just how critical this will be in strengthening our cyber resilience, and growing our ability to project power in cyberspace and to establish norms of responsible behaviour in cyberspace. We will never be complacent. As a key priority, I and my partner in GCHQ, Jeremy Fleming, urgently need the nation's cyber and digital talent, part time or full time. These cyberwarriors will be as vital to our defences as an F35 pilot, a special forces operator or a submariner – and in contact with the enemy more frequently and persistently than any of them.

Secondly, the pandemic has reminded us of the advantage conferred by being at the leading edge of science and technology. Our world-leading ability to conduct gene sequencing, identifying new variants of the virus and developing and deploying effective vaccines has – literally – meant the difference between life and death for tens of thousands of us. But as well as highlighting the opportunity it also demonstrates the peril in falling behind in the race to develop and exploit emerging and disruptive information age technologies.

We are confronted by a technological tsunami of which the most consequential include bio tech, QT, micro-electronics and semi-conductors, robotics and 5G. But the most significant, the 1st among equals, the one ring to rule them all, is Artificial Intelligence. Why? Because it is a new knowledge and reasoning system, it will be both foundational and an accelerant to every other field of emerging technology. It will become a pervasive and therefore decisive technology. We're not alone in making this assessment. In 2017, President Putin said that the nation that leads in AI will rule the world. China in particular is pursuing superiority in AI. Why does it matter to Defence? Well, as Eric Schmidt the former chairman of Google testified to congress recently, defending against AI capable adversaries without employing AI is an invitation to disaster.

AI will compress decision timeframes from minutes to seconds, expand the scale of attacks, and demand responses that will tax the limits of human cognition. Human operators will not be able to defend against AI-enabled cyber or disinformation attacks, drone swarms or missile attacks without the assistance of AI enabled machines. Even the best human operator cannot defend against multiple machines making thousands of manoeuvres per second at hypersonic speeds and orchestrated by AI across domains. Humans cannot be everywhere at once, but software can – it can augment human capability and can have enormous benefits. It can defend society and democracy, it can enable operational advantage, and remove humans from harm's way.

We are not starting from a low base – in 2019 the UK was ranked 3rd after the US and China in the global AI index. But that ranking conceals a huge gap in a winner takes all competition where first mover advantage is everything. The IR and the Defence Command Paper both cite AI as a strategic priority and a

thousand narrow AI flowers are blooming across Defence – but we have not mobilised this at the pace and scale needed.

We are putting the fundamentals in place beginning with an AI strategy, to be published this summer, and it will be guided by 3 main principles: (1) we will adopt and exploit AI for Defence at scale. (2) we will catalyse and strengthen the UK Defence and Security ecosystem for global leadership and (3) we will shape the global development of AI to support security, stability and democratic values. For Strategic Command, this begins with the establishment of a Defence AI centre this year as part of a wider digital ecosystem across Defence that we call The Foundry. And forgive me if I unashamedly get a bit techno techno, but the technology and the terms matter.

It will begin by integrating existing digital technologies now – for example using machine learning and automation to support Intelligence analysis. It will be enabled by improving our digital infrastructure – the digital backbone – with a data strategy that enables data curation, data sharing and data exploitation, cloud services at Secret and Above Secret, and a common network architecture. It will lead to investing in more S&T in partnership with DSTL and to experimentation to ensure responsible development of AI enabled and autonomous systems.

And above all it must mean building a talent pipeline with a Defence Digital Service and Digital Academy, with career fields in software development and data science. A career management system will nurture these rare talents across Defence – as well as growing a base of junior leaders in digital skills and computational thinking. The third lesson from the pandemic relates to this last point. As a society – whether in government, corporations or as individuals – we have adapted to the enforced changes brought about by lockdown at a pace that challenges all our previously conservative assumptions about how agile our organisations can be.

It shows that bold and radical change can be adopted and absorbed in our stride. Decisions in government that would normally take months or years were decided and implemented in hours. This rapid decision-making is only routinely seen during times of great crisis such as war, but this culture and mentality must become habit. We must be daring and entrepreneurial because the threat is moving towards us and the technological advantage away from us.

I want to turn now to the theme of this conference: Integration. As the Defence Secretary pointed out, two of the three seminal Defence related documents published this year contain Integration in the title. And last month in Honolulu, US Secretary of Defence Lloyd Austin described a concept of Integrated Deterrence echoing three of the principle conclusions of the Integrated Operating Concept and the Defence Command Paper.

First, as CDS has said, if you are up against rivals who seek to win without fighting, you cannot afford to be passive. In other words you have to compete below the threshold of war to deter war. And to prevent your adversaries from achieving their objectives in fait accompli strategies like those in Crimea and the South China Sea. Second, and hence my earlier comments on AI, our ability to innovate and develop a competitive edge in emerging disruptive

technologies will be fundamental – which is why sustaining strategic advantage through science and technology is integral to the strategic objectives in the IR. And third is that our ability to deter above and below the threshold of conflict will rise or fall on our ability to achieve Integration: of the levers of national power, across the five operational domains, and alongside allies.

But the key question we should be asking ourselves is who and what are we seeking to deter? Today's first panel session will explore this, but let me offer a trail. In his confirmation hearing to the US Congress in 1993, CIA Director James Woolsey characterised the threat as being composed of Dragons and Snakes. Both are still with us, only the Dragons are more powerful and malign and the Snakes are more prolific and diverse. Sometimes they act in concert. Some snakes cannot be deterred – they have to be suppressed or disrupted. This is why we will maintain cutting edge CT capabilities in our Special Operations Forces. Other snakes – like the Wagner Group for example or malicious cyber actors are used as proxies by the Dragons.

The largest Dragons in this metaphor are China and Russia. Russia is the acute and most menacing threat – the Defence Secretary described it as the number one threat to the UK just this Sunday. China is very different – a global power, a strategic rival and in some areas (we hope) a strategic partner. But our ability to manage this strategic rivalry requires the same tools of deterrence, modulated and applied to these Dragons in different ways.

Foremost among these is our ability to orchestrate our levers of national power, in a dynamic and persistent fashion, to contest the strategies both rivals are using against us. These strategies have been given a variety of labels: Hybrid Warfare, Liminal warfare, Grey Zone, Sub-threshold – the list is extensive, but they all describe the same essence. George Kennan captured this best in his telegram from Moscow in 1948. He used the term Political Warfare which he defined as: "The logical application of Clausewitz's doctrine in times of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives, to further its influence and authority and to weaken those of its adversaries. Such operations are both overt and covert." Kennan captured the weakness in our own approach which persists today. He wrote "…we have been handicapped however by a popular attachment to the concept of a basic difference between peace and war, by a tendency to view war as a sort of sporting contest outside of all political context."

It's not as if we don't recognise this. The comprehensive approach and fusion doctrine are both attempts better to integrate the levers of power. And it's not as if we haven't historically had the strategic culture. We have levers of national power that in each field rank among the most influential and extensive of any in the world: diplomatic, economic, legal, development, intelligence and security and defence. But our historically strong strategic culture has atrophied since the end of the cold war – it needs to be rekindled.

In some areas we do this well: our larger embassies overseas can be exemplars

of an integrated approach, responding dynamically to threats and opportunities and giving us significant influence and purchase. And the National Cyber Force is in many ways the perfect expression of the power of combining the different capabilities and operational cultures of government arms: the marriage of GCHQ, MOD, SIS and DSTL working to strategic priorities from the NSC is proving very potent.

But it's also fair to say that we have further to go in adapting the strategic machinery to the persistent and dynamic campaigning across Whitehall that the IR demands. We know it responds well in a crisis as it did following the poisoning of Sergey Skripal on British soil confirmed that, but it has yet to demonstrate it can campaign persistently and dynamically. The second facet of Integrated Deterrence is our ability to combine effects across all domains and all levels of warfare to create, find and exploit unprotected vulnerabilities and pose multiple dilemmas. And if needed to have the ability to impose cost in another domain entirely to the one an adversary is contesting.

This is Multi-Domain Integration – the precise role Strategic Command was established to lead and enable. Where each of the Services exist to conduct operations within their physical domains, we exist to conduct operations across and beyond them. That's why the Command holds the capabilities that allow Defence to sense, understand, orchestrate and enable effects across domains. There is no ready template for MDI and I have no easy answers, hence why we have drawn you together today to draw on your collective expertise and insight as we explore this further in the second panel. But we do know that our ability to develop the necessary expertise will hinge on a number of things and I want to touch on these.

First of all we will need to experiment and adapt as we harness new technology and new techniques. The hardware won't change between now and 2025 but the software will and our ability to exploit data with AI, establish a single information environment and extend our reach in cyberspace will allow us to push the boundaries of MDI with innovation and agility. We have established a formal programme of experimentation under AM Windy Gale, our new DG JFD, but the most valuable lessons will come from operations and here we have an inherent advantage with our special forces and PJHQ placed in the command. They are our vanguard and are already practising MDI, combining effects through cyberspace and space, with platforms and manoeuvre by air, land and sea to achieve cognitive and physical effects, overt and covert, in partnership with other government departments. It is happening on CSG 21 orchestrated by PJHQ and it is happening on special operations.

Secondly we need to change how we develop and field capability. The real source of military advantage lies less in platforms, it lies in our ability to sense, understand and orchestrate – in the kill chain as Christian Brose colourfully described it in his book of the same name: the sensor networks, the data, the PED and the effectors: kinetic or non-kinetic. But our requirements process is geared towards the acquisition of platforms, not to the networks that enable rapid decision-making across all levers of power. It is slow and We have a tendency to be impervious to disruption, lagging behind. We need to incentivise industrial partners by refreshing capabilities

constantly, develop strategic partnerships including with SMEs and develop a two-speed acquisition system that is fit for software DevSecOps, MVPs and with greater appetite for risk. The PUS is determined to unlock this and you can press him on it in the final session.

And third, MDI will require a cultural shift across Defence. We are still largely and recognisably a tri service organisation. Coordination across the services is still more of an afterthought than a reflex. We don't provide joint education until around the 15-20 year point in someone's career yet MDI expertise will be needed at every level including the most junior. Our approach to managing rare talent and skills that are needed across domains is still stove-piped, though our approach to managing cyber talent offers a model for how to change this.

Promotion and reward occur based primarily on how well you perform in your service, with service in joint (soon Integrated) posts of less import. An occasional paper published by RUSI and authored by Trevor Taylor and Andrew Curtis reminded us that as far back as 1964 Generals Pug Ismay and Ian Roberts advocated for greater integration in the MOD and between the Services than we see now. It's hard to avoid the conclusion that the requirement to develop expertise in MDI provides even more of an imperative now than it did then and I really welcome the fundamental reforms to our personnel strategy that are being pursued.

I haven't spoken about Integration with allies and partners. I've chosen not to partly because we have such excellent representation from the US and our colleagues in NATO on the panels, but mainly because it seems self-evident to me that the true source of our deterrent strength comes from the alliance and our close bilateral relationships with partner nations. That integration and the values we share and the respect for the Rules Based International System are what distinguish us from the Dragons and the Snakes.

At our inaugural conference last year I described the priorities I had for the IR: Cyber, Intelligence and Understanding, Special Operations and Multi-domain Integration and how they come together in Strategic Command to strengthen our deterrence and our competitive edge. These now lie at the heart of the Integrated Review outcome. We've been given the resources and the responsibility to lead the transformation of Defence for the Information age; we've now got to deliver.

Defence Secretary Strategic Command RUSI conference speech

It's all about integration today I noticed in the themes, and there's always a tendency to treat integration as the Holy Grail. And there are indeed champions of it who pursue integration for integration's sake with a sort of

purity that leads us into being exclusive rather than inclusive. And to do so would ignore the threat that we see today and the strengths that we in the West hold.

Let's start with what strengths we have – and what Russia doesn't have for example, and others – we have alliances. So integration must in my view be first and foremost about policy integration, campaigning integration, the culture of burden-share and playing to our strengths. An integrated response is what is demanded by today's threat. Multi-domain, broad action, inter-government, international relationships – sub-threshold and above threshold.

And next it must also mean interoperability – but not to the extent that we become over-dependent on one ally or another. And there are I'm afraid too many examples of that. The future of foreign policy and defence is in my opinion going to be bilateral, trilateral and small groups of countries with common cause. Of course, with one major exception – that being the tried and tested alliance of NATO.

So we have to be more generic, less exquisite. And lastly, and only lastly when it comes to integration, we need to find a way for our own forces to be more technically integrated, so we can dominate the kill chain, ISR process and exploitation of explosive actions on the battlefield, while at the same time allowing a range of partners to operate alongside. Easier said than done. But they must not do so at the expense of being deaf to those allies and their capabilities.

The challenge of achieving all three levels of this type of integration, with cybersecurity demands and multiple alliances, is not going to be an easy one. In fact, it will be harder if policy leads, equipment programmers and military leaders don't speak to each other, which is why at the Command Paper's heart is the threat. The start point is we coalesce around a common threat picture. We will begin to drive integration much better. It will become our demand signal that shapes our generators and partnerships.

While much of the media's focus on our paper was on the usual tired numbers game, many failed to notice the significant uplift in focus on defence diplomacy. Which is why Strategic Command is so important, and what it does in the next few years is set us up to deliver Global Britain. Better integration, a leader of culture and a leader of fast decision-making. What I expect to see from Strat Comm is also a step change in joint force development across Defence, both in the leaders and the culture, in its dynamic decision-making process and its response to the demand and the threat, and indeed influencing the equipment programme to make sure we have a better portfolio management of our requirements.

So I look forward to hearing Sir Patrick speak on how he's going to set about that. I look forward to seeing over the next few months how the Command Paper will be implemented by Strat Comm. Because Strategic Command has a really key, important place in this process. I visited it only the other week, no it was last week, the week before, time moves fairly fast these days. But what's key in that was everyone in that building worked on the process of an integrated purple joint interest in defence. They worked together no matter

what service they had come from. And I am afraid we still see in some of our other services, the single service view of the world. Well in today's threat, global competition we can't afford to have that anymore. We have to burden-share. We have to work with our partners. We have to find a way to weave in that integration. And it starts with the mindset of the policy leaders rather than technology.

DWP and Google join forces to grow jobseekers' digital skills

The scholarship will let jobseekers access courses to grow the necessary skills for a career in technology and IT, with Universal Credit claimants being referred to the scholarships by their Work Coach.

The courses do not require relevant experience or a degree and are recognised by industry experts and employers, including Google.

The courses which are now live to applicants include IT Support, Data Analyst, Project Manager and UX Designer.

Welcoming the announcement, Minister for Employment Mims Davies MP said:

> Helping jobseekers to build the confidence and skills they need to take up new opportunities is vital for the next stage in our recovery from the pandemic. Our Plan for Jobs puts skills at the heart of that and crucially Google's Career Certificates will help people showcase their digital skills and build our workforce of tomorrow.

Chancellor of the Exchequer Rt Hon Rishi Sunak MP said:

> Nothing is more important than helping people get new jobs. That is the mission of our Work Coaches day in and day out, and I'm delighted they'll be working with Google to give people the digital skills they need to do exactly that.

Ronan Harris, Google UK and Ireland's Managing Director, said:

> Technology must help everyone, no matter their location, race, age or education level. We must harness the opportunity to upskill people across the country for the jobs of the not so distant future.

> We hope that with these new efforts and the support of our public sector partners, even more people can develop the skills to thrive and continue growing their careers through technology.

Stephen Evans, Learning and Work Institute Chief Executive, said:

> As the economy reopens, so too will new job opportunities. For many of those looking for work, learning new skills will be a vital part of taking up these opportunities. This initiative has the potential to help jobseekers to gain the skills they need for a rewarding career and to do so in a flexible way.
>
> We must break down barriers to opportunity so everyone has the chance to make the most of their talents as we look to recover from the pandemic and build a prosperous future.

Julian David, techUK CEO, said:

> This initiative from Google, working with DWP, is another great way the technology industry is widening access to digital skills certifications that have a proven track record of leading to better employability and opportunity.
>
> Such courses provide flexible, affordable and effective routes for learners to acquire skills that are valued by employers which is crucial as we continue to support people into secure, resilient jobs.

Work Coaches will be able to combine these scholarships with additional tailored support on offer through the government's multi-billion-pound Plan for Jobs, aimed at protecting, supporting and creating jobs for people of all ages across the country.

The announcement follows an update this week, which showed that 100,000 jobseekers across Great Britain had started on the JETS Scheme – aimed at helping those that have lost jobs in the pandemic with their work search.

To help spearhead efforts to get people into work, the DWP has hired an additional 13,500 new Work Coaches, meaning people of all ages can access bespoke support to fire up their job hunt.

Media enquiries for this press release – 020 3267 5144

Follow DWP on:

Appointment of Commissioners of the Criminal Cases Review Commission

News story

Her Majesty The Queen, on the recommendation of the Prime Minister, has approved the appointment of Zahra Ahmed, Nicola Cockburn and Joanne Fazakerley as Commissioners of the CCRC.

Zahra Ahmed, Nicola Cockburn and Joanne Fazakerley have been appointed as Commissioners of the Criminal Cases Review Commission (CCRC) for 3 years from 1 June 2021.

The CCRC is an independent body, set up by the Criminal Appeal Act 1995, to investigate possible miscarriages of justice in England, Wales and Northern Ireland.

The CCRC decides if there is any new evidence or new argument which raises a real possibility that an appeal court would quash a conviction or reduce a sentence.

Appointments to the CCRC are regulated by the Commissioner for Public Appointments and comply with the Governance Code on Public Appointments.

Biographies

Zahra Ahmed

Zahra Ahmed is a practising barrister with specialist experience in regulatory, public law, immigration, and crime.

Zahra has a practice in the regulation of health care professionals. She provides legal advice and recommendations on the disposal of cases, in order to assist regulators in discharging the duty to protect the public. Zahra presents cases before professional disciplinary panels and she has previously

worked as an in house lawyer at the General Pharmaceutical Council.

Zahra has been instructed by the Crown Prosecution Service, the Serious Fraud Office and as Junior Counsel to the Undercover Policing Inquiry

Nicola Cockburn

Nicola Cockburn is Judge of the First-tier Tribunal, Immigration and Asylum Chamber.

Joanne Fazakerley

Joanne Fazakerley is a solicitor and is currently a consultant at Paul Crowley & Co Solicitors. Previously, Joanne was a solicitor at Hogan’s Solicitors.

Published 26 May 2021