

# Compliance Newsletter

March 2021

*Compliance News for Customer People*

## Contemptible, Clueless or Inept?

- **The ICO's on a £1.2m fining frenzy (but it's not all about the GDPR)**
- **Is being clueless better than being inept? Discuss**
- **BA data breach case looms with giddy hopes of a £2.4bn payout**
- **ASA finds that advertisers are still targeting junk food, booze and weight loss products at children online**
- **FCA's demands more protection for the vulnerable and plans to police the funeral plan 'wild West'**
- **The Guardian's exclusive reveal's contact centre giant's PR disaster home worker monitoring plans**
- **5 key questions to ask your tech provider in order to keep you cyber secure**

This month we delve into exactly who's getting fined by the ICO during its current enforcement flurry - and why. As well as the usual canter around the world of customer experience compliance and regulation. Read on to find out more.

**Welcome to our 21<sup>st</sup> newsletter:**



Information Commissioner's Office

## The Leads (Don't) Work and Pulled Muscles as the ICO ramps up enforcement and fines

By the start of March the ICO had levied fines on 11 companies for breaking the marketing laws in 2021, just one less than the total for the whole of 2020.

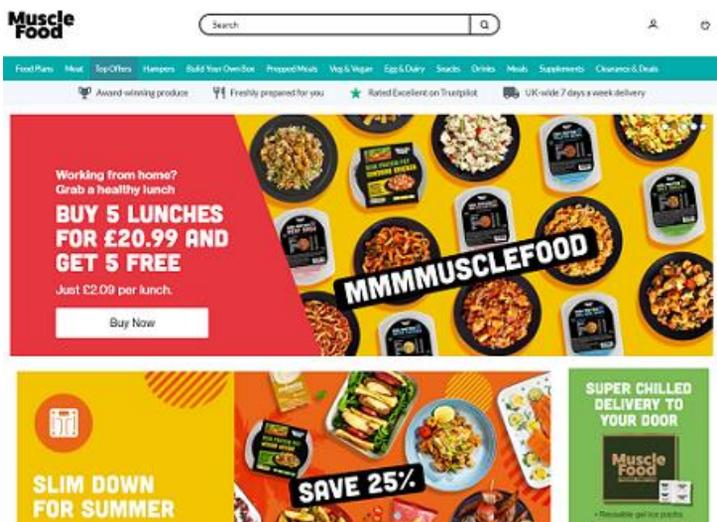
The two latest fines were of a pair of widely contrasting firms.



**Leads Work** is a lead generating organisation that generated a record volume of consumer complaints to the SMS text 7726 complaints service. The 3 million texts were sent using the Avon brand, but weren't directly authorised by Avon as they were to help field sales agent recruit sub-agents to work on their behalf.

“In lockdown and want to earn extra cash? Avon is now FULLY ONLINE, FREE to do and paid weekly. Reply with your name for info. 18+ only. Text STOP to opt out.”

However, Leads Work had no clear consent to do so and as the ICO identified “no mitigating factors” in the case, it [fined LW £250,000](#).



**Muscle Foods** is a subsidiary of [DB Foods](#) ("the UK's leading independent wholesaler of meat, poultry, game, deli and sundry supplies"). DB's turnover is in the 9 figures; it's a substantial, well-resourced organisation. Unfortunately, that didn't stop Muscle Foods sending over 135 million illegal emails and 6 million texts to consumers advertising its foods and food supplements. In its ruling announcing a [£50,000 fine](#), the ICO highlighted that Muscle's *online checkout journey did not make it clear that customers would receive subsequent marketing communications*, made worse by Muscle not stopping its marketing efforts while the ICO carried out its investigation.

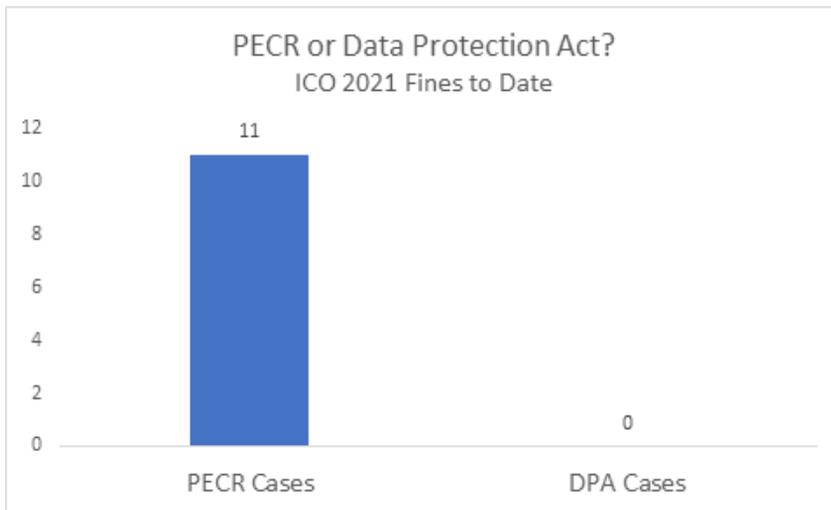
### **New Fines, Same Old Rules**

Although both firms were operating in very different markets, they were equally guilty of pretty fundamental errors and illegal activity in their consumer marketing.

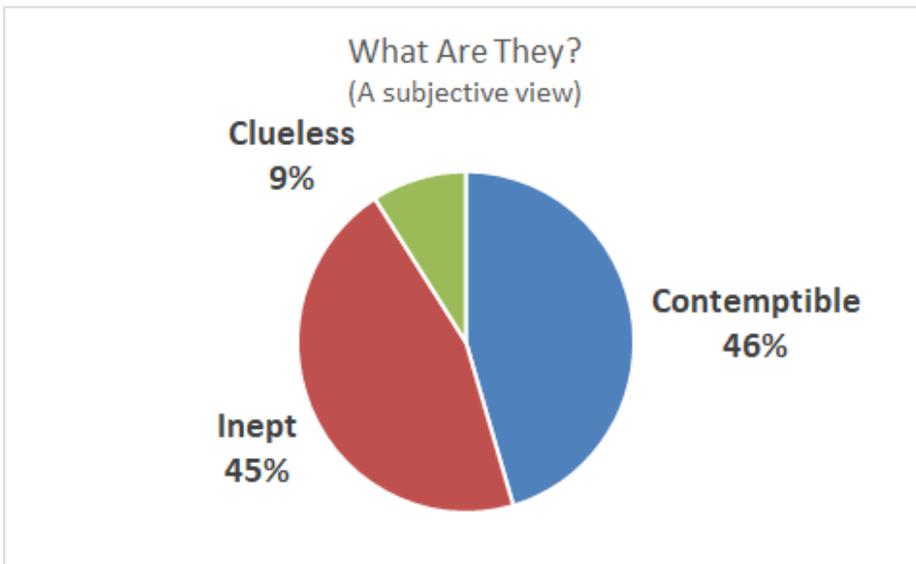
But the ICO wasn't making use of the GDPR and the 2018 Data Protection Act (DPA) when bringing them to book. No, all 11 fines so far this year have been for companies breaking the nearly 20 years old PECR (Privacy and Electronic Communication Regulation) rules.

The rules on phone, email and SMS consent, etc, should be very well understood by now. So, why do these fundamental mistakes continue to be made? Especially when they are typically made by firms that - either because of their size or their role in sales and marketing services - should definitely know better.

We decided to do a bit of analysis...



**What's 46% contemptible, 45% inept and 9% clueless? The ICO's fined felons, that's what**



Read the full article [here](#).

Youth fashion site, [Just Hype](#) (not heard of it, grandad?) also made a ill-advised move into the selling of (fashionable) face masks. Hundreds of thousands of promotional SMS messages were sent by Just Hype, both to previous customers whose checkout journey wouldn't have led them to understand they would receive marketing texts and 3rd parties who had no relationship with or awareness of Just Hype at all (which was blamed - like so much in life - on an unnamed "IT Consultant").

The [ICO has fined Just Hype £60,000](#) and acknowledged various changes it has made to its internal processes and customer communications.

## £2.4bn - A case of hope over expectation



Invigorated by the ICO's £20m fine of BA for its 2018 data breach, the 'Group Litigation Order' (class action) being organised to seek compensation for BA customers exposed to the breach continues. The deadline to join in is the end of April, but I can't help but feel that estimates of a pay out of up to £2.4bn are a bit on the optimistic side.

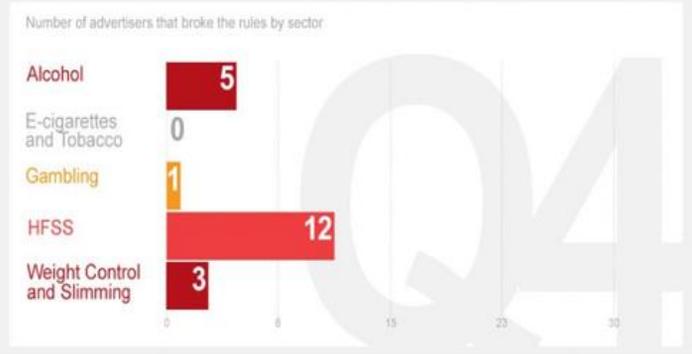
## Calm Across the Channel, Stormy Over the Atlantic - A 2 Minute Data Protection Re-Cap

Here's a [quick-read](#) article we wrote earlier this month for Sheffield's finest, the Contact Centre Panel.





### How many advertisers were caught breaking the rules in October – December 2020?



The ASA's sweep of websites and YouTube has shown that advertisers are still [breaking the rules](#) by placing ads for adult goods and services where children are likely to see them. All the advertisers have been made to remove their ads - and for once BrewDog doesn't seem to have pushed its way onto the naughty step.



Privacy Policy | Feedback | Follow @MOL | Saturday, Mar 27th 2021 12AM 9°C @ 3AM 9°C @ 5-Day Forecast

# MailOnline News

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Video | Travel | DailyMailTV | Discounts

Latest Headlines | Covid-19 | Royal Family | Crime | Boris Johnson | Prince Harry | Meghan Markle | World News | Headlines | Most read | Login

## Argos will refund more than £500,000 to 114,000 customers in e-card vouchers after breaking rules over extended warranty

- Argos will refund £570,010 in total to 114,002 customers in £5 e-card vouchers
- Retailer broke rules on extended warranty deals for more than a year, CMA found
- Sainsbury's owned chain failed to remind shoppers of options to shop around
- Shoppers who bought warranties for electrical products online will be contacted

By MARK DUELL FOR MAILONLINE  
PUBLISHED: 11:28, 26 March 2021 | UPDATED: 18:07, 26 March 2021

Share | 34 View comments

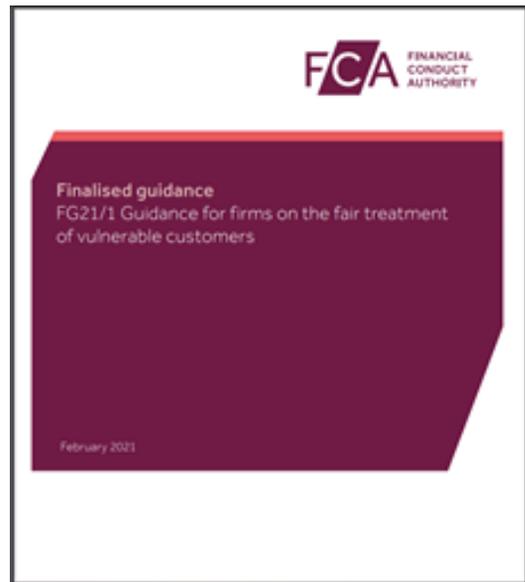
The CMA has [forced Sainsbury's-owned Argos](#) to refund over 100,000 customers after failing to be open and transparent with them when selling extended warranties on electrical goods. Although as Argos is giving refunds via £5 e-cards then the redemption rate will probably be so low that it will be a bargain sanction for Argos.

## Updated Vulnerable Consumer Guidance

The FCA's long-awaited [updated guidance](#) on the fair treatment of vulnerable customers has been published.

The new requirements - which include the expectation that fair treatment of vulnerable customers is both 'led from the top' and baked into firms' processes - include:

- Understand the needs of its target market/customer base
- Ensure staff have the right skills and capability to recognise and respond to the needs of vulnerable customers
- Respond to customer needs throughout product design, flexible customer service provisions and communications
- Monitor and assess whether they are meeting and responding to the needs of customers with characteristics of vulnerability and make improvements when this is not happening



## RIP for Dodgy Funeral Plan Sales?

The FCA has published a [consultation](#) on how it will regulate the Pre-Paid Funeral Plan sector once it ceases to be self-regulated and falls under the FCA's jurisdiction in July 2022. The consultation is a hefty 355 pages long, but key planned changes from a 'customer' perspective are:

- An end to sales through 'cold calling'
- Stopping up front commission payments (up to £900) for funeral plan sales intermediaries
- A requirement for funeral plan firms to truly understand, audit and manage their sales supply chains, including lead generation

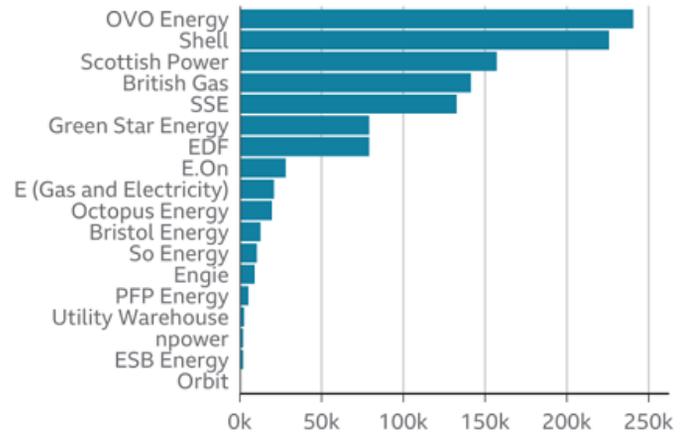
All of which will signal massive change in the existing sector's structure, processes and business models.



Over a million energy customers will be [refunded](#) after suppliers inadvertently overcharged them through the transition from old provider to new.

### More than 1m customers overcharged in switching failures

Number of customers affected by supplier



Source: Ofgem



## Homeworking Webinar Series

### Webinar 1 - Ensuring a secure and productive homeworking environment

17 February 2020 | Clients: 12.00 - 12.45 | Outsourcers: 13.00 - 13.45

**Topics for discussion**

- Data security**
  - Identifying the risks in a non structured environment
  - Taking secure payment from a home environment
- Data protection**
  - Regulatory considerations and contractual obligations
- Connecting workers securely to core data systems**
  - BYOD - creating safe access from personal devices
  - Securing end points

**Panel**

- Simon Turner (QSA)**  
PCI DSS Advisory Cloud  
Services & Contact Centres  
BT Plc
- John Greenwood**  
Head of Technology & Payments  
Contact Centre Panel
- Steve Sullivan**  
Head of Regulatory Compliance  
Contact Centre Panel
- Brent Agar**  
Director - North America  
SentryBay

### Secure & Productive Homeworking Webinar

Our friends at Contact Centre Panel recently kindly asked me to join their panel to discuss Secure & Productive contact centre homeworking - and followed it up with this [summary article](#).

## PR Corner

Global contact centre outsourcing giant [Teleperformance](#) won't have enjoyed [this story](#) from last weekend's [Guardian](#).



The screenshot shows the top of a Guardian news page. The header includes 'Support the Guardian' with 'Contribute' and 'Subscribe' buttons, and the Guardian logo. The main article is titled 'Call centre staff to be monitored via webcam for home-working 'infractions'' by Peter Walker. The sub-headline reads 'Exclusive: Teleperformance, which employs 180,000 people, plans to use specialist webcams to watch staff'. A sub-headline below that says 'Missing from desk: AI webcam raises remote surveillance concerns'. The article features a photo of a person wearing a headset. To the right of the article is an advertisement with the text 'From "no idea"' and a small graphic.

Just now, most contact centre employers are grappling with the performance, morale and ethical challenges of managing and supporting a hybrid or solely-home based workforce. There are plenty of tech providers eager to fill the 'command and control' gap created by the move from more traditional work models.

However, Teleperformance's plans to deploy a webcam solution that *"monitors and tracks real-time employee behaviour and detects any violations to pre-set business rules, and sends real-time alerts to managers to take corrective actions immediately"* hasn't gone down well with employees, The Guardian (which, ironically, uses Teleperformance's services in the UK) or - presumably - clients and other stakeholders.

In the article the firm denied that it had any plans to use the technology with UK staff. But it still announced the 'big brother' regime - which would identify unrecorded breaks, or lengthy pauses in typing & talking and so on - to UK colleagues and warned the presumed whistle-blower that their revelation amounted to gross misconduct.



**Dealing with new ways of working**

Moving your business online will present some new risks, placing more reliance on digital technologies such as web hosting, credit card processing, and productivity tools like email, video and chat.

You shouldn't need a degree in computer science for your small business security, but, cyber security is complicated. If you don't have all the IT skills yourself, it can be hard to know what to do - and when you're done enough. Having good relationships with your IT service provider(s) will help massively with this. So we've identified and explained the key cyber security topics we think you should care about, so you can be sure you're covering all the right bases.

© Crown Copyright 2020

### 1. Assess the cyber security of your business

Consider if the measures you take to deal with the lockdown will become more permanent ways of working. For example, will you look to expand your online business? If so, you'll need systems which are sustainable and can scale as your business adapts and grows.

### 2. Establish a baseline

Answering the questions below will give you a good idea of your security status, and identify what areas need attention. The NCSC's Cyber Essentials scheme provides a way to demonstrate to others that you have good security in place.

-  **What IT products and services do you use? Is your job to look after these, or a service provider's?**
-  **Some insurance policies now include a basic level of cover for cyber risks. This can be useful if you suffer an incident. Review your policies to understand the level and type of cover (if any) that is provided.**
-  **Are you using cloud services? The NCSC's cloud guidance can help you choose secure products, and use them safely.**
-  **Do you have access to IT support? As you become more reliant on digital services, think about how you'd cope if these were unavailable.**
-  **Are there any regulations you need to follow? If your business is now processing Personally Identifiable Information (PII) online, you will need to sign up on GDPR. If you are processing card payment information, the Payment Card Industry Data Security Standard will apply.**

### 3. Talking to your IT service providers

If you are talking directly with your supplier, the following questions will help you ensure that security is at the forefront of any new service you decide to take on.

-  **Patching & Updates:** Ask your suppliers how often they patch the services you use, and check any contracts or SLAs to ensure that patching is included.
-  **Backups:** What sort of back up arrangements are in place and how often are these backed up? You should know how often your data is backed up, where it is stored, and who has access to it.
-  **Access:** Is your data (and the data of others which you have responsibility for) being properly protected? Are you able to put 2FA in place to limit access to your data and services?
-  **Logs:** Are logs being kept for security purposes? Logging can play a vital role in diagnosing any problems. Logs will also prove invaluable after responding to and recovering from security incidents.
-  **Incident Response:** What will happen if things go wrong? Service providers should operate on the presumption that they will be attacked. It should be clear how and when they will engage with you during a security incident.

**Find out more**  
For more information about how to improve cyber security within your organisation, please read the NCSC web pages especially for small businesses at [www.ncsc.gov.uk/smallbusiness](http://www.ncsc.gov.uk/smallbusiness).

[www.ncsc.gov.uk](http://www.ncsc.gov.uk) | [@NCSC](#) | [National Cyber Security Centre](#) | [@cyberhel](#)

**Infosec and Cyber Security - What questions to ask your techies**  
Our friend and all-round business resilience and continuity guru Julie Goddard of [Humanex Resilience](#) shared this really useful, practical [infographic](#) from the National Cyber Security Centre (NCSC). It's primarily designed for small businesses, but it is useful for 'customer people' in all sorts of organisations.

**PSA**

Phone-paid Services Authority

**FR** FUNDRAISING REGULATOR

**Ofwat**

**Ofcom**

All quiet this month for Ofcom, Ofwat, PSA and the Fundraising Regulator.

**The Small Print**

This content is accurate as of 28<sup>th</sup> March 2021.

Channel Doctors is a trading name of Murphy Sullivan Associates Limited, a company registered in England and Wales with Registration Number 4830889.

Subscribe here <http://eepurl.com/gqxzw5> and you will receive the next edition direct to your in-box