HENDERSON CHAMBERS

Alerter

Regulatory and Cybercrime

3 April 2020

Workchain: unauthorised data access is a serious offence for companies and their officers

By Beatrice Graham and Tim Green

As the Coronavirus causes unprecedented and rapid change in our daily lives and many of us get used to the challenges of remote working, it is a good time to remind clients of the recent CoA decision in *R. (on the application of Pensions Regulator) v Workchain Ltd* [2019] EWCA Crim 1422 which demonstrates the wide application of the Computer Misuse Act 1990 ("CMA"). The case serves as a stark warning for companies and their officers who are not taking data security seriously. Tim Green was instructed by The Pensions Regulator ("TPR").

Change brings innovation

1. The **CMA** received Royal Assent 7 years before wireless internet was commercially available and 17 years before Apple launched the first iPhone. It might then not seem immediately obvious to use the distinctly "analog" CMA as an effective weapon in the prosecution of modern digital data misuse and cybercrime. However, recent case law suggests the CMA is an Act of Parliament whose time has come. In particular, *Workchain* shows how the creation of imprisonable offences under the CMA is now highly relevant in the regulation of companies and individuals committing unauthorised access to data for commercial gain.

The Facts

2. The prosecution of Workchain Ltd arose out of the following facts: Workchain was an employment agency and the company, its directors and 5 area managers accessed, without authorisation, the data of its employees in order to opt-out these workers from the statutory workplace pension scheme. Workplace pension schemes deliberately use an opt-out model whereby workers are automatically enrolled into a workplace pension unless the worker makes the deliberate choice to opt-out of their workplace pension. This makes planning for a secure retirement the default position. Companies are required to match the employee's contribution, which is taken at source.

3. To achieve the opt-out, Workchain accessed worker's pensions data held by the National Employment Saving Trust ("**NEST**") without the permission of the NEST using personal details supplied by worker to Workchain as their employment agency (eg national insurance numbers, DOBs, etc). By ensuring workers opted-out of their workplace pensions, Workchain would have reduced the company's outgoings long-term and affected the long-term security of many 'temp' workers, many of whom were already in a precarious state of employment.

CMA and the prosecution of corporates

4. Practitioners will know how it can be difficult to prosecute companies successfully because of the identification doctrine for proving the companies state of mind, specifically where dishonesty has to be proved to the criminal standard such as for Fraud Act offences. In this case, a prosecution for fraud would have been made more complicated by the fact that some employees for Workchain had consented to being opted-out and, given temporary nature of the work, many had moved on and/or disappeared and so could not be asked to provide evidence.

5. Instead of attempting the fraud route, the TPR indicted the defendants under s1 CMA for unauthorised data access relating to the workers' confidential pensions data held by NEST. The basic CMA offence attracts a maximum 2-year prison sentence and an unlimited fine on conviction on indictment. Confiscation would also have been an available power because the case was indictable. The aggravated offence pursuant to s2 CMA of unauthorised data access with intent to commit a further offence carries a maximum of 5 years imprisonment.

The ingredients for a successful Computer Misuse Act 1990 prosecution

6. S1 CMA only requires proof that a person (a) uses a computer to perform a function with intent to access data and (b) that the access is unauthorised and (c) they know it to be unauthorised. There is no need to prove the authorised data access was dishonest or was with some ulterior intent, only that the defendant committed the unauthorised access and at that time he knew it was not authorised by the data controller. This makes the offence an attractive one to use against companies such as Workchain and potentially much larger corporates.

7. The evidence in this case was clear. The Financial Controller and HR & Compliance Officer, among others, rang NEST posing as their temporary workers in order to access employee NEST ID numbers. These were then used to login to the individual workers' accounts and 'opt-out' of the scheme. NEST did not authorise the access to workers' data and became suspicious. NEST then alerted TPR which noticed the large number of workers opting out from Workchain figures. Phone recordings made by Workchain managers were examined and an investigation launched.

8. The CMA proved a powerful weapon and, following a long investigation, all eight defendants including Workchain and its directors pleaded guilty to s1 CMA. The case was committed to Derby Crown Court where a substantial sentencing hearing lasting 4 days before HHJ Shant QC, the Recorder of Derby, who heard evidence and argument about the level of culpability and harm. HHJ Shant QC then imposed a fine of £250,000 on Workchain and prison sentences on the directors.

9. In the absence of any sentencing guidelines and relevant case law, the Judge proceeded to basis her sentence on first principles pursuant to sections 142 and 143 of the CJA 2003.

10. She considered first the victim's financial loss and the offender's financial gain, then the numbers affected and whether the losses, even if small, were significant to those individuals. She then moved onto public interest, particularly the damage done by undermining public trust in computer systems of this nature. Further factors considered included, *inter alia*, the reasons for the unauthorised access and the position of trust. Finally, discounts had to be made in the light of mitigation and early pleas of guilty.

The Appeal

11. Workchain appealed the fine to the CoA. In the first Judgement of the CoA concerning data crime committed for economic gain, the CoA upheld the Judge's overall approach to the sentence of the Recorder of Derby. At paragraph 43 of the Judgement the CoA held:

> "*Workchain's culpability was clearly high. Its senior employees unlawfully attempted to persuade its workers to opt out and, having failed to do so, pretended to be those workers in order to access unauthorised data for the purposes of defeating the automatic enrolment provisions of the scheme set up by the 1990 Act. The conduct was successful, as shown by the high rate of opt outs achieved, compared with the norm.*"

12. Notwithstanding the CoA having sympathy for the sentencing Judge's approach, taking into account the guilty plea and giving weight to its mitigation, the CoA reduced the fine from £200,000 to £100,000.

Workchain and data security in the digital economy

13. The CoA's decision Judgement in Workchain is important reading for practitioners in data and cyber regulation. A link to the Judgement can be found **here**. The relevant principles to be taken from the case can be summarised in this way:

    a. *The basic CMA offence does not demand an ulterior intent and so is easier to prove, particularly against corporates, than some other offences*.

    b. *In the absence of a definitive sentencing guideline for this type of offending, the Court will have regard to the generic sentencing guidelines and proceed from first principles*. No other sentencing guidelines, such as that for fraud, is analogous. Workchain is now the leading authority for data crime.

    c. *An attack on data security should not be dismissed as abstract.* Here Workchain abused their position of trust and, in so doing, risked the integrity of a carefully considered government opt-out policy and the security of employees already vulnerable as temporary workers.

    d. *Company officers convicted of even the basic offence can expect a prison sentence.*

    e. *The financial value of a fraud such as this is not the determining factor of its seriousness.* It is notable that the sums Workchain avoided paying were relatively insignificant. However, the gravamen of the offence lay in the deliberate attack on workplace pensions and undermining public confidence in the data held. This justified a fine of £100,000 even with an early guilty plea.

f. *Legislation in the cyber security space already exists that can be applied with great effect when considered in a new light*. Even as technology advances, the law is not necessarily always playing catch up. The case represents an interesting use of the CMA, which has previously been thought of as a tool in blackmail and industrial terrorism space.

14. Home working was growing in popularity even before the emergency created by COVID-19 and this trend is likely to increase in the months to come. Practitioners and clients need to be mindful both of the need for data security and also the enforcement powers available to the public or private prosecutor should a data be misused for economic gain.

Please follow the links for more about the authors Beatrice Graham and Tim Green

3 April 2020