Information Commissioner's Office

DATA PROTECTION ACT 2018 (PART 6, SECTION 155)

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

TO: Tuckers Solicitors LLP

OF: 39 Warren Street, London, W1T 6AF

1. Tuckers Solicitors LLP ("Tuckers") is a limited liability partnership, which is authorised and regulated by the Solicitors Regulation Authority (No. 592449) and registered in England and Wales (Companies House No. OC382272).

2. The Information Commissioner ("the Commissioner") has decided to issue Tuckers with a Penalty Notice under section 155 of the Data Protection Act 2018 ("the DPA"). This penalty notice imposes an administrative fine on Tuckers, in accordance with the Commissioner's powers under Article 83 of the General Data Protection Regulation 2016 ("the GDPR")[1]. The amount of the monetary penalty is £98,000.

3. The monetary penalty has been issued because of a contravention by Tuckers of Articles 5(1)(f) of the GDPR. The Commissioner finds that, during the period of 25 May 2018 to 25 August 2020 ("the relevant period"), Tuckers failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss,

[1] The applicable legislation at the time of the Incident was the (EU) GDPR. The Commissioner was at the material time the supervisory authority in respect of the (EU) GDPR.

destruction or damage, using appropriate technical or organisational measures.

4. Tuckers became aware on 24 August 2020 of a ransomware attack on its systems, and on 25 August 2020 determined that the attack had resulted in a personal data breach. The Commissioner considers that Tuckers' failure to implement appropriate technical and organisation measures over some or all of the relevant period rendered it vulnerable to the attack. The attack resulted in the encryption by the malicious and criminal actor (the "attacker") of 972,191 individual files, of which 24,712 related to court bundles; of the encrypted bundles, 60 were exfiltrated by the attacker and released in underground data marketplaces. The compromised files included both personal data and special category data.

5. In addition, whilst not forming the basis of the substantive contravention, the Commissioner is also concerned by Tuckers compliance over the relevant period with Articles 5(1)(e), 25, 32(1)(a) and 32(1)(b) GDPR.

6. In the interests of clarity, 25 May 2018 is the date when GDPR came into effect, and 25 August 2020 is the date on which Tuckers reported the breach to the Commissioner and shut down the relevant system, preventing any further possible authorised access.

7. This Monetary Penalty Notice explains the Commissioner's decision, including the Commissioner's reasons for issuing the monetary penalty and for the amount of the penalty.

Legal framework for this Monetary Penalty Notice

Obligations of the controller

8. Tuckers is a controller for the purposes of the GDPR and the DPA, because it determines the purposes and means of the processing of personal data held on its computer systems (GDPR Article 4(7)).

9. 'Personal data' is defined by Article 4(1) of the GDPR to mean:

> *information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

10. 'Processing' is defined by Article 4(2) of the GDPR to mean:

> *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

11. Controllers are subject to various obligations in relation to the processing of personal data, as set out in the GDPR and the DPA. They are obliged by Article 5(2) to adhere to the data processing principles set out in Article 5(1) of the GDPR.

12. In particular, controllers are required to implement appropriate technical and organisational measures to ensure that their processing of personal data is secure, and to enable them to demonstrate that their processing

is secure. Article 5(1)(f) ("**Integrity and Confidentiality**") stipulates that:

> *Personal data shall be […] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*

13. Article 5(1)(e) ("**Storage Limitation**") provides, in material part:

> *Personal Data shall be […] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed […]*

14. Article 25 ("**Data protection by design and by default**") provides, in material part:

> *1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet*

the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons

15. Article 32 ("**Security of processing**") provides, in material part:

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) […]

(d) […]

2. *In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

3. *[…]*

The Commissioner's powers of enforcement

16. The Commissioner is the supervisory authority for the UK, as provided for by Article 51 of the GDPR.

17. By Article 57(1) of the GDPR, it is the Commissioner's task to monitor and enforce the application of the GDPR.

18. By Article 58(2)(d) of the GDPR, the Commissioner has the power to notify controllers of alleged infringements of GDPR. By Article 58(2)(i) he has the power to impose an administrative fine, in accordance with Article 83, in addition to or instead of the other corrective measures referred to in Article 58(2), depending on the circumstances of each individual case.

19. By Article 83(1), the Commissioner is required to ensure that administrative fines issued in accordance with Article 83 are effective,

proportionate, and dissuasive in each individual case. Article 83(2) goes on to provide that:

> *When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
>
> *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
>
> *(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
>
> *(e) any relevant previous infringements by the controller or processor;*
>
> *(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and*

mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

20. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner. Section 155 of the DPA ("**Penalty Notices**") provides that:

(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 149(2) …,

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR.

21. The failures identified in section 149(2) DPA 2018 are, insofar as relevant here:

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

…;

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors)e[…]

22. Schedule 16 includes provisions relevant to the imposition of penalties. Paragraph 2 makes provision for the issuing of notices of intent to impose a penalty, as follows:

> *"(1) Before giving a person a penalty notice, the Commissioner must, by written notice (a "notice of intent") inform the person that the Commissioner intends to give a penalty notice."*

The Commissioner's Regulatory Action Policy

23. Pursuant to section 160(1) DPA, the Commissioner published his Regulatory Action Policy ("RAP") on 7 November 2018.

24. The process the Commissioner will follow in deciding the appropriate amount of penalty to be imposed is described in the RAP from page 27 onwards. In particular, the RAP sets out the following five-step process:

a. Step 1. An 'initial element' removing any financial gain from the breach.
b. Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2) - (4) DPA.
c. Step 3. Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.
d. Step 4. Adding in an amount for deterrent effect to others.

e. Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

Factual background to the incident

25. Tuckers' website describes it as the UK's leading criminal defence lawyers specialising in criminal law, civil liberties and regulatory proceedings. Established in 1983, the firm has numerous offices in Greater London, Greater Manchester, West Midlands, Kent, Sussex, Staffordshire and Somerset.

26. On 24 August 2020 Tuckers determined that it had been subjected to a ransomware attack; parts of its IT system became unavailable. Upon investigation, its IT staff identified a ransomware note from the attacker stating that they had compromised Tuckers' system.

27. On 25 August 2020 it submitted a personal data breach notification to the Commissioner. It explained that the attack had resulted in the encryption of civil and criminal legal case bundles stored on an archive server. Backups were also encrypted by the attacker. The Commissioner notes that these actions by the attacker affected only the archive server; the vast majority of the personal data Tuckers was processing was in fact held on other servers and systems that were not affected by the attack.

28. Tuckers stated that a significant number of personal data records were held on the archive server and provided the total number of encrypted files as a result of the attack.

29. In total, 972,191 individual files were encrypted. Of these, 24,711 related to court bundles. Of the 24,711 court bundles, 60 were exfiltrated by the attacker and published on an underground market site (the "dark web").

30. Tuckers stated that the bundles included a comprehensive set of personal data, including medical files, witness statements, name and addresses of witnesses and victims, and the alleged crimes of the individuals. The 60 exfiltrated court bundles included 15 relating to criminal court proceedings and 45 civil proceedings. Of the 60 exfiltrated court bundles, the personal data was not related to just one living individual; it was likely to have included multiple individuals.

31. In respect of the criminal cases, Tuckers stated it included one ongoing criminal case at the Proceeds of Crime Act Stage, the criminal trial had concluded. All other criminal cases had been concluded. In respect of the civil cases, Tuckers explained that there was a mixture of archived and live cases. The Commissioner notes that some of the personal data compromised by the attack was likely to have featured in open court proceedings, but the unauthorised access to personal data resulting from this attack was very different in nature and scale. Tuckers further explained that to its understanding the personal data breach has not had any impact on the substance of its archived or live cases, i.e. on the conduct or outcome of the relevant proceedings.

Overview of the attack

32. The attack resulted in the unavailability of personal data (via encryption) and a loss of confidentiality (via access to, and exfiltration of, the personal data).

33. On 27 August 2020 Tuckers commissioned third-party investigators, [redacted], to provide a 'Cyber Security Incident Response Report'. Neither Tuckers nor [redacted] was able to determine conclusively how the attacker was able to access Tuckers' network. However, it did find evidence of a known system vulnerability [redacted] that could have been used to either access the network, or further exploit areas of Tuckers once inside the network.

34. [redacted] released a patch for [redacted] in January 2020. Tuckers has told the Commissioner that it applied the patch in June 2020, but it has accepted that the attacker could have exploited it during the five-month unpatched period[3].

35. Once inside the network, the attacker installed various attacker tools which allowed the attacker to create its own user account, which it did. The attacker used this account to execute the attack and encrypt a significant volume of personal data contained in case bundles held on the archive server within the Tuckers network (see paragraph 29 above). As well as encrypting the personal data and the backups, the attacker also exfiltrated 60 court bundles and released them onto the dark web.

36. Tuckers notified all but seven of the parties detailed within the 60 court bundles which had been released[4]; this was done in line with the

[2] 'CVE' is a reference number used to identify known vulnerabilities.
[3] It is noted that Tuckers' own GDPR & Data Protection Policy states that *"all software, operating system and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities".*
[4] These seven had been subject to a custodial sentence when Tuckers last had contact with them. Tuckers stated that they therefore did not have a postal address for these individuals at any stage; either because they did not have one before they were remanded to custody and/or they only had a relationship with them in custody, so did not record any address outside of prison.

requirements of Article 34 GDPR. It also made a public notification of the incident using its social media presence and its website.

37. Tuckers provided an update to the Commissioner on 7 September 2020 stating that it had moved its servers to a new environment and the business was now back to running as normal, albeit without the restoration of the data that had been compromised by the attacker. It stated that, whilst the compromised court bundles were effectively permanently lost, the material within the bundles was still available on its case management system which was unaffected by the attack.

38. The Commissioner has considered whether these facts constitute a contravention of the data protection legislation.

The Contravention

39. For the reasons set out below, and having carefully considered Tuckers' representations, the Commissioner has concluded that Tuckers contravened Article 5(1)(f) GDPR. The Commissioner makes clear that he accepts that primary culpability for this incident rests with the attacker. But for the attacker's criminal actions, regardless of the state of the security, the breach would not have occurred. However, the infringements identified by the Commissioner were relevant to the personal data breach because they gave the attacker a weakness (vulnerability) to exploit and/or because they increased the risks to personal data once the attacker entered Tuckers' network. Particularly in light of the volume and nature of the personal data for which Tuckers were responsible, data security contraventions that created such risks were serious matters that justify enforcement action on the facts of this case.

40. In reaching those conclusions, the Commissioner has given consideration to Article 32 GDPR, which requires a controller when implementing appropriate security measures to consider "*the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*".

41. As part of his deliberations, the Commissioner has considered, in the context of "state of the art", relevant industry standards of good practice including the ISO27000 series, the National Institutes of Standards and Technology ("NIST"), the various guidance from the ICO itself, the National Cyber Security Centre ("NCSC"), the Solicitors Regulatory Authority ("SRA"), Lexcel and 'NCSC Cyber Essentials'.

42. The Commissioner has concluded that there are a number of areas in which Tuckers has failed to comply with, and to demonstrate that it complied with, Article 5(1)(f) GDPR. Tuckers' technical and organisational measures areas were, over the relevant period, inadequate in the following particular respects:

- **Lack of Multi-Factor Authentication ("MFA")**

43. Tuckers explained that it used a [redacted] environment to deploy remote desktops via the [redacted] web app and that its [redacted] environment was at the centre of the cyber-attack. Its GDPR and Data Protection Policy required two-factor authentication where available, however, it stated that it did not use Multi-Factor Authentication (MFA) for its [redacted] remote access solution.

44. With regards to "state of the art", the Commissioner notes that ISO27002 recommends "*where strong authentication and identify verification is*

required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometrics should be used".

45. NIST 800-63b requires that where *"some assurance"* is needed that the individual authenticating is who they claim to be, authentication may be allowed via a single factor such as password. Where a high degree of certainty is required, controllers should implement either MFA or a combination of two single factor authenticators. Where a very high degree of certainty is required, authentication should be based on proof of possession of a key through a cryptographic protocol including possession of two distinct authenticators.

46. The Commissioner understands that [redacted] published guidance in 2016 which stated that organisations should not use single factor authentication for [redacted] in production environments. The NCSC has recommended since 2018 to use MFA for services such as remote access. It says that MFA is particularly important for authentication to services that hold sensitive or private data. The NCSC Cyber Essentials requires multi-factor authentication where it is available, and the SRA also published guidance in 2018 which recommended the use of MFA where possible.

47. The Commissioner believes that the use of MFA was a comparably low-cost preventative measure which Tuckers should have implemented, with there being a number of both open and proprietary/commercial MFA solutions widely available that are compatible with[redacted].

48. The use of MFA substantially increases the difficulty of an attacker entering a network via the exploitation of a single username/password. Had MFA been used, it could have substantially supported Tuckers in preventing access to its network. The Commissioner is cognisant of the fact that Tuckers is unable to confirm exactly how the attacker entered its

network – however, the exploitation of a single username and password is a common exploitation method and is likely to be one of two possible entry methods into the Tuckers network. The lack of MFA accordingly created a substantial risk of personal data on Tuckers' systems being exposed to consequences such as this attack.

49. Taking into consideration the highly sensitive nature of the personal data that Tuckers was processing, as well as the state of the art of MFA, and the costs of implementation, Tuckers should not have allowed access to its network using only a single username and password. In doing so, it did not ensure appropriate security, including protection against unauthorised and unlawful processing of its personal data, as required by Article 5(1)(f) GDPR.

50. For the same reasons, the Commissioner considers that Tuckers also failed to meet the requirements of Article 32(1)(b) which required appropriate measures to be put in place to ensure the ongoing confidentiality, integrity and availability of its data processing systems and services.

- **Patch Management**

51. Following [redacted], [redacted] proceeded to check the state of the [redacted] environment. [redacted] provided a number of commands to validate whether a [redacted] had been compromised via the vulnerability, one of which showed "significant indication" of this. [redacted] released a mitigation step for this vulnerability on 19 December 2019. It provided a patch to fix the vulnerability on 19 January 2020. Tuckers stated to the Commissioner that it installed the patch in June 2020, more than four months after the patch was released,

and accepted that the attacker could have exploited its vulnerability during the un-patched period.

52. With regards to "state of the art", it is apparent that [redacted] had announced on 17 December 2019 that it was aware of the vulnerability CVE-[redacted] and provided mitigation steps to prevent exploitation of it, with a patch to fix the vulnerability being released on 19 January 2020. At the time of becoming aware of the vulnerability, [redacted] advised in a published security bulletin on its website that it "*strongly urges affected customers to immediately upgrade to a fixed build OR apply the provided mitigation which applies equally to* [redacted] *and* [redacted] *deployments".*

53. On 27 January 2020, the NCSC published an 'Alert' that malicious actors were exploiting the CVE-[redacted] vulnerability. The Alert said *"the NCSC recommends following vendor best practice advice to mitigate vulnerabilities. In this case, the most important aspect is to install the latest updates as soon as practicable and to follow the vendor mitigation advice immediately[…] the NCSC also strongly advises organisations carry out searches across their networks to identify whether exploitation has taken place".* It provided a link to a tool that detects the vulnerability. On 29 January 2020, the NCSC published a subsequent Alert on its website. It provided further details on how to detect the vulnerability.

54. On 8 April 2020, the NCSC published a joint advisory with the US Department of Homeland Security (CISA) titled "*COVID-19 exploited by malicious cyber actors".* It explained that CVE-[redacted] and its exploitation has been widely reported online since January 2020; it provided links to guidance on how to resolve the vulnerability.

55. On 28 April 2020, [redacted] published a security blog drawing attention to recent ransomware attacks. It explained that malicious actors were exploiting such vulnerabilities as remote access without multi-factor authentication, older operating systems such as 'Server 2008' and the [redacted] vulnerability CVE-[redacted].

56. The Commissioner has considered relevant industry standards of best practice, including the ISO27002 suggestion that organisations should define a timeline to react to notifications of potentially relevant technical vulnerabilities, and once a vulnerability has been identified, associated risks should be identified and actions taken, such as patching the system to remove the vulnerability.

57. The Commissioner understands the CVE scored a CVSS[5] of 9.8: A score of 9.8 is rated as "critical". The 'NCSC Cyber Essentials' requires patches that are rated as 'high' or 'critical' should be applied within 14 days of the release of the patch. As stated, the patch was released in January 2020 and installed some five months later. In addition to the NCSC Cyber Essentials, the ICO's Security Outcomes guidance also recommends actively managing software vulnerabilities and the application of software update patches.

58. The SRA also published guidance in 2018 which highlighted the importance of maintaining up-to-date IT equipment/systems.

59. In terms of cost, the patch was available for free. The Commissioner accepts that whilst the cost of the patch was free, there are other cost implications, such as the cost of personnel to test the patch prior to deployment. However, in the Commissioner's view, this should not have

[5] The CVSS is an independent rating scale on how critical a vulnerability is. The CVSS scale is based on low, medium, high and critical, based on scores from 0 to 10.

been a barrier to the prompt application of the patch given the sensitive personal data being processed.

60. Taking into consideration the highly sensitive nature of the personal data that Tuckers were processing, as well as the state of the security updates, and the costs of implementation for them, Tuckers should not have been processing personal data on an infrastructure containing known critical vulnerabilities without appropriately addressing the risk. In doing so, it did not ensure appropriate security, including protection against unauthorised and unlawful processing of its personal data, as required by Article 5(1)(f) GDPR.

61. The Commissioner further notes that Tuckers' own GDPR & Date Protection Policy states that *"all software, operating system and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities".* Tuckers speculated that it was unlikely the attacker would have exploited a vulnerability to gain access to the network, but then not executed the attack until August 2020, two months after initial access. However, this is a common attacker tactic used by advanced persistent threat groups. Accordingly, the Commissioner is not persuaded that the passage of time from June 2020 (when the patch was implemented) and August 2020 (when the attacker exfiltrated data) casts significant doubt on the likelihood of this patching delay having given the attacker the opportunity they exploited. In any event, even if the attack did not exploit this delay, the delay was nonetheless a significant deficiency in Tuckers' technical measures that created the risk of serious incidents such as this.

62. For the same reasons, Tuckers also failed to meet the requirements of Article 32(1)(b) which required appropriate measures to be put in place to

ensure the ongoing confidentiality, integrity and availability of its data processing systems and services.

- **Failure to encrypt personal data**

63. Tuckers provided information during the Commissioner's investigation that the personal data stored on the archive server that was subject to this attack had not been encrypted. The Commissioner accepts that encryption of the personal data may not have prevented the ransomware attack. However, it would have mitigated some of the risks this attack posed to the affected data subjects. This is because effective encryption management, with appropriate protection of the decryption keys, can prevent an unauthorised party such as a malicious attacker from being able to read the personal data once they have obtained access to systems. Such encryption would therefore have upheld the principles of confidentiality of the personal data, even in its exfiltrated form.

64. With regards to "state of the art", The Commissioner has taken into consideration relevant standard of best practice, including the ISO27001 requirement to implement cryptographic controls in compliance with all relevant agreements, legislation and regulation. NIST 800-53 also discusses how the selection of cryptographic mechanisms should be based on the need to protect the confidentiality and integrity of organisational information. It says that the strength of a mechanism should be commensurate with the security category or classification of the information. The Commissioner understands that the Tuckers GDPR and Data Protection Policy identified client data as its most sensitive data, requiring the highest level of protection.

65. The Commissioner's published guidance on encryption also states that it "*considers encryption to be an 'appropriate technical measure', and in*

cases where data is lost or unlawfully accessed and encryption was not used, we may consider regulatory action". The ICO's Security Outcomes guidance suggests implementing technical controls such as encryption to prevent unauthorised or unlawful processing of personal data. The SRA also published guidance in 2017 which highlights encryption as a cost-effective step in keeping information safe.

66. Although the ICO does not endorse or recommend one particular encryption solution, the Commissioner understands that free, open-source encryption solutions are widely available, or, should Tuckers have wished to purchase specific court-bundling software with encryption capabilities, this is also commercially and inexpensively available. The Commissioner's experience is that the use of encryption solutions is an industry norm within legal services, as would be expected.

67. Taking into consideration the highly sensitive nature of the personal data that Tuckers were processing, as well as the state of the art of encryption, and the costs of implementation, Tuckers should not have been storing the archive bundles in unencrypted, plain text format. In doing so, it did not ensure appropriate security, including protection against unauthorised and unlawful processing of its personal data, as required by Article 5(1)(f) GDPR.

68. For the same reasons, Tuckers also failed to meet the requirements of Article 32(1)(a), which expressly cites the encryption of personal data as an appropriate security measure.

Notice of Intent

69. On 7 September 2021, in accordance with s.155(5) and paragraphs 2 and 3 of Schedule 16 DPA, the Commissioner issued Tuckers with a Notice of

Intent to impose a penalty under s.155 DPA. The Notice of Intent described the circumstances and the nature of the personal data breach in question, explained the Commissioner's reasons for a proposed penalty, and invited written representations from Tuckers.

70. On 22 November 2021, Tuckers provided substantial written representations in respect of the Notice, together with supporting documentation in relation to its finances. In answer to further questions posed by the Commissioner on 1 December 2021, Tuckers provided additional information on 24 December 2021.

71. On 7 February 2022, the Commissioner held a 'representations meeting' to thoroughly consider the representations provided by Tuckers. At that meeting it was decided that a monetary penalty remained appropriate in all of the circumstances.

Factors relevant to whether a penalty is appropriate, and if so, the amount of the penalty

72. The Commissioner has considered the factors set out in Article 83(2) of the GDPR in deciding whether to issue a penalty for the contraventions of Article 5(1)(f) (and 32(1)) particularised above. For the reasons given below, he is satisfied that (i) the contraventions are sufficiently serious to justify issuing a penalty in addition to exercising his corrective powers; and (ii) the contraventions are serious enough to justify a significant fine.

(a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

73. The Commissioner considers that there have been a number of infringements identified in relation to Articles 5(1)(f) GDPR that have demonstrated Tuckers' approach to data protection compliance was not of an appropriate standard.

74. In its public communication of the breach, it stated that it held client information relating to over 60,000 clients. Tucker stated that, during the attack, a significant amount of personal data, including special category data, was unlawfully accessed and encrypted by the attacker. This included over 20,000 court bundles, of which 60 bundles were exfiltrated and released onto the dark web.

75. The personal data included within the bundles included special category data, and related to individuals that were particularly vulnerable, including children and individuals involved in significant crimes. This, in the Commissioner's view, increases the severity of this infringement, given that this type of personal data required particularly high levels of security to be applied to it.

76. In terms of the duration of the infringement, the Commissioner considers that the contravention period for this breach persisted over at least part of the period from 25 May 2018 (i.e. the date on which GDPR came into force) until 25 August 2020 (i.e. the date on which Tuckers reported the breach to the Commissioner and shut down the relevant system, preventing any further possible authorised access). The Commissioner notes that Tuckers failed to have MFA in place, which was recommended from at least 2016; it resolved this issue by 19 November 2020. As explained above, the patch management contravention spanned the period from January to June 2020. The encryption contravention is likely to have persisted over a longer period.

77. In terms of the assessment of damage suffered by affected data subjects, the Commissioner has regard to Recital 85 GDPR which explains that "*physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned*".

78. The Commissioner finds that the release of personal data of the type in this case on to the dark web in particular, is likely to increase distress to the affected individuals, not least given the vulnerability of some of the individuals to whom the data related.

79. Some of the exfiltrated data includes image files in relation to allegations of [redacted], and bundles that identify the complainants; documents which identify [redacted] and [redacted]; and the [redacted] of witness to crimes. In some instances, the compromised data included legally professionally privileged information between clients and Tuckers.

80. Further, the exfiltrated data included personal data relating to a prisoner's child (in relation to access to the child). Recital 38 GDPR explains that children merit specific protection with regard to their personal data. The child's privacy has been breached, with intimate details of their family life published online.

(b) the intentional or negligent character of the infringement

81. The Commissioner considers that this personal data breach occurred due to a criminal and malicious cyber-attack that exploited negligent security practices.

82. Tuckers were aware prior to the attack that its security was not at the level of the NCSC Cyber Essentials. In October 2019, it was assessed against the 'Cyber Essentials' criteria and failed to meet crucial aspects of its requirements.

83. The NCSC describes Cyber Essentials as: "*A simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks[…] Cyber attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked. Our advice is designed to prevent these attacks".*

84. Given the personal data that Tuckers was processing, including special category data of very vulnerable individuals, the Commissioner believes that it is reasonable to expect that the security within Tuckers should have not only have met, but surpassed the basic requirements of Cyber Essentials. The fact that some 10 months after failing Cyber Essentials it had still not resolved this issue is, in the Commissioner's view, sufficient to constitute a negligent approach to data security obligations.

85. In addition, Tuckers were accredited by the Law Society's Lexcel Legal Practise Quality Mark. Its March 2018 Standards stated that law practises should be accredited against Cyber Essentials. This further reinforced the conclusion that Tuckers should have had the requisite measures in place to achieve accreditation by at least October 2019, and when it failed its Cyber Essentials assessment, it should have quickly and promptly resolved the inadequacies. Had it done so, it could have demonstrated a

much stronger approach to compliance and would have greatly reduced the likelihood of this personal data breach from occurring.

86. Tuckers is also regulated by the SRA. In 2017, the SRA warned its organisations that the legal sector was an obvious target for cyber criminals. It stated that "*solicitors are obliged under the Code of Conduct to maintain effective systems and controls to mitigate risks to client confidentiality".*

87. It also provided security guidance in 2017, in its "*IT Security: keeping information and money safe*" publication; and in 2018, in its "*Technology and Legal Services*". Both provided advice and guidance, such as encryption, secure remote access and up to date operating systems and software, that if followed, would have significantly reduced the likelihood of this attack being successful.

88. In addition, the Commissioner provided free assessment tools kits for controllers to use to support them in complying with the GDPR. One such toolkit (regarding 'Records Management') provided advice and guidance on deleting personal data when it is no longer necessary (i.e. when the retention period has expired).

89. Further negligent practices by Tuckers that were of concern to the Commissioner included:

- Failing to implement MFA on its [redacted] remote access solution. [redacted] advised in 2016 that you should have MFA in place for production environments, and the NCSC recommended in 2018 that you should have MFA in place for remote access solutions.

- Processing personal data on the operating system [redacted], which ended mainstream support in 2015, and ended extended support in January 2020, meaning that it was no longer supported, and therefore received no security updates.

- Not applying a high-risk security patch until four months after it was released, despite it being listed as 'critical'. This was particularly negligent given that the NCSC had published an Alert drawing attention to it.

- Failing to apply encryption techniques to data at rest, despite ICO Guidance from 2018 recommending it;

- Storing court bundles after its 7-year retention period, some of which were exfiltrated through this attack. A failure to adhere to or to justify departures from its retention practices creates concerns about compliance with Article 5(1)(e) GDPR, which requires personal data to be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"*[6].

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

90. Tuckers assessed that, in relation to the individuals of the 60 exfiltrated court bundles, these were likely to result in a high risk to individuals;

[6] Tuckers stated to the Commissioner at one point during his investigation that *"this is where criticism of us is most justified and where we are looking to rebuild our systems without repeating the sins of the past. We have been reasonably good at managing our case management environment and central archives on the basis that we do not store items for longer than necessary where possible. However, the files that were accessed were in locations that were not being proactively managed well enough with regards ensuring that data that was still being stored outside of our retention periods was then being deleted".* The Commissioner notes, however, that subsequent representations from Tuckers suggested that its retention of the compromised files was justified.

therefore, in line with Article 34 GDPR requirements it notified the affected data subjects of the personal data breach[7], using the following methods: letters and emails sent on 19 October 2020; social media notification; and website publication.

91. In addition, Tuckers commissioned third party support (i.e. [redacted]) who provided incident response support following the breach. It also reported the incident to Action Fraud, the National Crime Agency, the Metropolitan Police, the NCSC, and the SRA.

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

92. The Commissioner is also satisfied that Tuckers was responsible for multiple breaches not only of Article 5(1)(f) but also of Article 32, not least through its failure to implement MFA on its remote access solution and its patch management inadequacies. The Commissioner finds that Tuckers failed to meet the requirements of Article 32(1)(b) GDPR, which required appropriate measures to be put in place to ensure the ongoing confidentiality, integrity and availability of its data processing systems and services. In relation to the lack of encryption of the archived court bundles, Tuckers failed to meet the requirements of Article 32(1)(a) GDPR, which lists the encryption of personal data, inter alia, as an appropriate security measure.

(e) any relevant previous infringements by the controller or processor

[7] Save for the 7 individuals for whom Tuckers had no contact details for (see Footnote 3).

93. The Commissioner is unaware of any previous data protection infringements by Tuckers.

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adve effects of the infringement

94. Tuckers were fully cooperative with the Commissioner's investigation.

(g) the categories of personal data affected by the infringement

95. The compromised bundles contained a range of categories of personal data, and special category data as defined by Article 9(1) GDPR. Specifically those categories included:

- *Basic Identifiers*
- *Health Data*
- *Economic and Financial Data*
- *Criminal Convictions*
- *Data revealing racial or ethnic origin*

96. Given the nature of court bundles, however, the personal data affected by this attack was not confined to discrete fields such as those listed above. Instead, the data included narrative descriptions of facts, allegations and opinions about the data subjects referred to in those bundles. In total, 972,191 individual files were encrypted. Of these, 24,711 related to court bundles which contained a wide range of personal data. Of the 24,711 court bundles, 60 were exfiltrated by the attacker and published on the dark web. Of these 60 bundles, 45 related to civil cases and 15 related to criminal cases.

97. In relation to the civil proceedings, Tuckers stated that "*the bundles are bundles that were prepared by us – but again bundles that were prepared for use in connection with either a preliminary or final hearing in relation to the matters. In civil proceedings it is our responsibility (we do only Claimant work) to prepare the bundles for use in connection with the Court hearings*."

98. In relation to the criminal proceedings, Tuckers stated that "*all the material is material that was served on Tuckers by the prosecution and would therefore have been subject to use in open Court proceedings. The bundles do not include any documentation that we have prepared, for example letters providing legal advice or draft statements prepared in connection with the defence. It is only prosecution evidence served on us – which includes documentation and videos relating to CCTV/Body Worn Video served on*". The Commissioner has given weight to the fact that some of the compromised data will have been referred to in open court proceedings, but does not consider that this eliminates the serious prejudicial consequences of this attack, which resulted in extensive and sensitive data being made available to unauthorised persons in ways that are very different from references in court during the course of proceedings.

99. Tuckers explained that the bundles included a comprehensive set of personal data, including medical files, witness statements, name/addresses of witnesses and victims, and alleged crimes, including particularly heinous crimes such as rape and murder.

100. It stated that some of the clients involved in its cases are vulnerable in terms of their mental or physical wellbeing, with such information being included as part of those clients' bundles.

101. It confirmed that witness statements were contained in many of the compromised bundles.

102. Tuckers provided the Commissioner with a summary of each of the exfiltrated bundles, which included personal data relating to vulnerable individuals as well as very sensitive personal data, including:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

103. Tuckers notified the Commissioner via a self-reported personal data breach form on 25 August 2020, one day after becoming aware of the

security incident, and the same day that it determined the security incident had resulted in a personal data breach.

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

104. Not applicable.

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

105. Not applicable.

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

106. The Commissioner has considered the following **aggravating factor** in this case:

- The Commissioner's Regulatory Action Policy states that "*In data protection cases, whether the relevant individual or organisation is certified by a body that has been accredited under Article 43 of the GDPR or has failed to follow an approved or statutory code of conduct*", the commissioner reserves the right to take this into consideration as an aggravating factor.

  The SRA has a published 'Code of Conduct for Firms'. Of particular relevance here are the requirements to: [Para 2.1(a)] "*Have effective governance structures, arrangements, systems*

and controls in place that ensure […] [compliance] with all the SRAs regulatory arrangements as well as with other regulatory and legislative requirements, which apply to you"; [Para 2.5] *"[…]identify, monitor and manage all material risks to your business"*; [Para 3.1] *"[…] keep up to date with and follow the law and regulation governing the way you work"*; and [Para 5.2] *"[…]safeguard money and assets [including documents] entrusted to you by clients and others"*.

The Commissioner considers that Tuckers has failed to meet these standards of the Code.

107. The Commissioner has considered the following **mitigating factors** in this case:

- Tuckers has proactively sought to address the security concerns and engaged with third party experts to increase the security of its systems, including

  (a) On 19 November 2020 it completely separated from its legacy infrastructure and updated to a [redacted] environment;

  (b) It implemented MFA access to all other remote access environments;

  (c) It has purchased database and software capabilities as a service where [redacted] will be responsible for updating and patching the core infrastructure, database and software;

(d) It is engaging with 'Cyber Griffin' at the City of London Police and has made it mandatory for all of its employed staff to attend their baseline briefings;

(e) It has also agreed to invite 'Cyber Griffin' to do an audit of its security procedures prior to applying again for Cyber Essentials in the first instance and, Cyber Essentials Plus shortly thereafter;

(f) It is in the process of completing its purchase of licences from [redacted] to run [redacted] on their user accounts, in order to provide greater security in relation to the devices that connect to its network; it has also engaged the services of a [redacted] network engineer to support them in configuring this. Once this is done it intends to apply for NCSC Cyber Essentials Accreditation;

(g) It has automated the deletion of personal data within its case management system on the expiry of the retention period. For personal data stored outside its case management system, it is using an external consultant to identify tools built into its new [redacted] environment that will support the classification, and automated deletion, of personal data.

(h) It has encrypted data on Tuckers' systems through [redacted] and [redacted] encryption. This is so by design.

(i) It has transferred all client data to [redacted] which has ensured the effective application of Tuckers' data retention policy to all such data

(j) It has continued to improve training and information security awareness throughout its business, including through weekly communications on cyber risks and awareness. This, in turn, has led to the increased reporting of suspicious activity, thereby improving the security of Tuckers' systems

(k) It has made improvements to the management of Tuckers' antivirus and privileged accounts, with local admin end users having been removed.

(l) It has addressed the human resourcing issues and now utilises a third-party specialists as required and has expanded its IT team. There are now four members of staff including a Systems Manager who is responsible for ensuring that all third-party contracts and services that Tuckers uses for specialist support are well managed

(m) Penetration testing has been carried out and is regularly scheduled. All critical and high-risk issues identified in those tests have been remedied

Summary and amount of penalty

108. For the reasons set out above, the Commissioner has decided to impose a financial penalty on Tuckers. The Commissioner has taken into account the size of Tuckers, publicly available information regarding its finances, and the representations made by Tuckers as to its financial position. He is mindful that the penalty must be effective, proportionate and dissuasive.

Calculation of the penalty

109. Following the 'Five Step' process set out in the RAP the Commissioner has arrived at an appropriate penalty amount as follows:

Step *1: An initial element removing any financial gain from the breach*.

110. The Commissioner noted that there was no financial gain or benefit to Tuckers from this breach.

***Step 2: Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) DPA*.**

111. This refers to and repeats the matters listed in Article 83(1) and (2) as set out above. The breach was a negligent one which involved personal data of those individuals linked to court cases for criminal and civil proceedings. The affected personal data involved (but was not limited to) basic identifiers, financial and economic data and other special category data. The Commissioner has outlined above a number of failings identified in respect of Tuckers' steps to take appropriate organisational and technical measures. These failings resulted in 972,191 individual files being encrypted. Of these, 24,711 related to court bundles which contained a wide range of personal data. Of the 24,711 court bundles, 60 were exfiltrated.

112. The Commissioner acknowledges Tuckers' cooperation throughout the investigation, and the steps taken by Tuckers to contact the individuals affected by the breach in line with Article 34 GDPR.

113. The duration of the infringement was up to 2 years and 3 months, though the precise period varied between the particular contraventions.

114. Based on the above, the Commissioner finds that the starting point for any penalty in respect of this breach is 3.25% of Tucker's annual turnover for 30 June 2020.

Step 3: Adding in an element to reflect and aggravating factors (Article 83(2)(k)).

115. The Commissioner notes Tuckers' failure to comply with the SRA code of conduct, but has not applied any increase to the penalty percentage of 3.25% in this instance.

Step 4: Adding an amount for deterrent effect to others.

116. No increase has been applied for this factor in this instance.

Step 5: Reducing the amount to reflect any mitigating factors including ability to pay.

117. Prior to serving the Notice of Intent, the Commissioner noted the steps taken by Tuckers to avoid future breaches in light of this incident (including purchase of software, automated deletion, implementation of MFA and staff training). He believed that these were processes which should have been in place in any event, and applied no reduction for this.

118. The Commissioner has gone on to consider the extensive representations made by Tuckers in response to the Notice of Intent, including representations made in respect of the proposed penalty sum and the impact of a penalty on the firm. The Commissioner is satisfied that

Tuckers has submitted significant representations regarding the circumstances of the incident and the subsequent further remedial measures implemented following the breach, including:

- Additional IT staff members
- Increased training and professional penetration testing

119. The Commissioner has also considered:

- Tuckers financial position
- Additional information which was provided which narrowed the scope of the Commissioner's findings in relation to the contravention
- Representations made in relation to managing IT staff illness/shortages
- The important work Tuckers do in protecting vulnerable individuals
- Further clarification that the infringements identified were purely in relation to Tuckers' archive system

120. Taking into account all of the factors set out above, the Commissioner has decided to impose a penalty on Tuckers of **£98,000** (**ninety-eight thousand pounds**).

Payment of the penalty

121. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by **29 March 2022** at the latest. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

122. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

(a) The imposition of the penalty; and/or,

(b) The amount of the penalty specified in the penalty notice

123. Any notice of appeal should be received by the Tribunal within 28 days of the date of this penalty notice.

124. The Commissioner will not take action to enforce a penalty unless:

- the period specified within the notice within which a penalty must be paid has expired and all or any of the penalty has not been paid;

- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and

- the period for appealing against the penalty and any variation of it has expired.

125. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

126. Your attention is drawn to Annex 1 to this Notice, which sets out details of your rights of appeal under s.162 DPA.

Dated the 28th day of February 2022

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

Rights of appeal against decisions of the commissioner

1. Section 162 of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:e

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   Telephone: 0203 936 8963
   Email: grc@justice.gov.uk

a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:e

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;

h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).