DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Life at Parliament View Limited

Of: Regina House, 124 Finchley Road, London NW3 5JS

1. The Information Commissioner ("Commissioner") has decided to issue Life at Parliament View Limited ("LPVL") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is being issued because of a serious contravention of the Seventh Data Protection Principle by LPVL.

2. This notice explains the Commissioner's decision.

Legal framework

3. The DPA implemented European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The DPA must be applied so as to give effect to that Directive. Both the DPA and the Directive have since been repealed, but the contravention at issue in this case took place while they were still in force.

4. LPVL is a data controller, as defined in section 1(1) of the DPA in respect of the processing of personal data. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, it is the duty of a

data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

5. The relevant provision of the DPA is the seventh data protection principle which provides, at Part I of Schedule 1 to the DPA, that:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

6. Paragraph 9 at Part II of Schedule 1 to the DPA provides that:

"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to –

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected".

8. Under section 55A (1) of the DPA the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the DPA by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

9. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

Background to the case

10. LPVL, trading as 'LiFE Residential', describes itself on its website as an estate agency offering services in lettings, sales and property management.

11. In March 2015 LPVL integrated with a partner organisation which offered a property letting transaction service. A component of the integration process required the transfer of tenant data held on LPVL's server to the partner organisation.

12. In order to share and sync files with its partner organisation, LPVL set up a File Transfer Protocol (FTP) server. The Commissioner understands the FTP server had previously been used to transfer property photographs to another system, and that an agreement was reached jointly between LPVL, its systems provider, and the partner organisation to repurpose this FTP.

13. LVPL indicated that it had intended the FTP to feature Microsoft Basic Authentication, which would require a username and password in order to allow file transfers. LVPL configured the FTP following online guidance available on Microsoft's website, which was wholly inappropriate for the task LVPL was seeking to accomplish, given that it allowed 'anonymous access' and also did not require encrypted communications.

14. In following this guidance, LVPL inadvertently misconfigured the server in relation to access controls, leaving a function known as 'Anonymous Authentication' switched on. This permitted any individual to access the server and the data of tenants without taking authentication steps, such as username and password, from 4 March 2015 onwards. Access restrictions were not implemented, so that all users, including

anonymous users, had full access to the data stored on the server. The FTP server was further misconfigured in that whilst approved data transfers were encrypted, personal data transmitted to non-approved parties was not. As such, transfers of personal data over FTP to non-approved parties had the potential to be compromised or intercepted in transit.

15. The exposed data on the server comprised 60 different document categories, of which 52 contained personal data. LPVL informed the Commissioner that the personal data of 18,610 unique individuals was placed at risk.

16. The types of personal data potentially compromised included names, phone numbers, e-mail addresses, postal addresses (current and previous), dates of birth, income/salary, employer details (position, company, salary, payroll number start date, employer address & contact details), accountant's details (name, email address & phone number). It also contained images of passports, bank statements, tax details, utility bills and driving licences of both tenants and landlords. The majority of this information dated from 2014 onwards.

17. On 15 February 2017, the vulnerability was identified whilst LPVL was conducting a review of the files on the server and immediate remedial action was undertaken.

18. During the period of vulnerability (4 March 2015 – 15 February 2017) LPVL confirmed that there had been 511,912 anonymous user logon events from 1,213 unique IP addresses recorded in the FTP server logs. The vast majority of these were repeated connections from the same IP addresses, which it was suspected had been carried out programmatically.

19. LVPL has confirmed that the unique IP addresses detailed in paragraph 18 above issued a number of FTP commands, including deletion, uploading, creation and removal of folders, and file renaming.

20. On 2 October 2017, LPVL was contacted by an individual who identified themselves as a hacker. This individual claimed to possess information relating to LPVL's customers and issued a threat to release information if a ransom was not paid. The individual also produced evidence indicating that the personal information to which they had referred had been accessed from the compromised server prior to detection and remediation of the vulnerability.

21. The Commissioner has made the above findings of fact on the balance of probabilities.

22. The Commissioner has considered whether those facts constitute a contravention of the DPA by LPVL and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

23. The Commissioner finds that LPVL contravened the following provisions of the DPA:

24. LPVL failed to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data in contravention of the Seventh Data Protection Principle at Part I of Schedule 1 to the DPA.

25. LPVL also failed to comply with the requirements set out in paragraph 9 at Part II of Schedule 1 to the DPA.

26. The Commissioner finds that the contravention was as follows:

LPVL did not take steps to ensure that personal data on its network was secured to a suitable standard due to gaps in the technical and organisational measures in place at the time of the incident, in particular:

- LPVL used an inappropriate and insecure method to facilitate access/transfers of large quantities of personal data to a third party;
- The above failing was compounded by LVPL's misconfiguration of the FTP server, which left large quantities of personal data exposed to unrestricted and unauthorised access. Even if user names and passwords were enabled, this would not have secured the data to a suitable standard;
- Post configuration of the server, LVPL failed to monitor access logs, conduct penetration testing or implement any system to alert LPVL of downloads from the FTP server, which would have facilitated early detection and containment of the breach;
- Failure to provide staff with adequate and timely training, policies or guidance either in relation to setting up the FTP server, or information handling and security generally.

This was an ongoing contravention until LPVL took remedial measures on 15 February 2017.

27. The Commissioner is satisfied that LPVL was responsible for this contravention.

28. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

29. The Commissioner is satisfied that the contravention identified above was serious.

30. This is because the personal data of over 18,000 individuals was placed at risk. Whilst the data involved was not in itself sensitive, the nature and type of personal data potentially compromised was sufficiently wide ranging to enable identity and/or financial fraud.

31. Furthermore, given LPVL's failure to detect the vulnerability until a review of its IT system in February 2017, the data was exposed for a period of almost two years. During this period, the data involved was accessed over half a million times by over one thousand unauthorised IP addresses, when modifications and alteration of some of the data took place, thereby reducing its integrity.

32. In the circumstances, the Commissioner considers that the contravention was serious having regard to the wide ranging nature of the personal data involved and the potential consequences, the number of affected individuals, the duration of the contravention, and the fact that personal data was accessed and substantially amended on multiple occasions by unauthorised users.

33. The Commissioner is therefore satisfied that condition (a) from section 55A (1) DPA is met.

Contraventions of a kind likely to cause substantial damage or substantial distress

34. The relevant features of the kind of contravention are:

Wide ranging personal data of tenants (and to a lesser degree landlords) could be accessed by unauthorised third parties over a period of almost two years.

35. The Commissioner considers that the contravention identified above had the following potential consequences:

36. The contravention would cause distress to the data subjects whose confidential and personal data has been disclosed to a recipient who has no right to see that information.

37. Further, the data subjects would be distressed by concerns that their data has been further disseminated, even if those concerns do not actually materialise.

38. If this information has been misused by those who had access to it, or if it was disclosed to untrustworthy third parties, then the contravention would cause further distress and also substantial damage to the data subjects such as exposure to the risk of identity and/or financial fraud.

39. The Commissioner has been unable to establish whether any of the leaked data is still publicly available, given that it comprised mainly scanned documents, which makes it difficult to run searches to locate the data. The Commissioner considers that the distress suffered by data subjects as described above would be exacerbated by concerns

that the data may still be in the public domain. This would especially be the case in relation to some identity related documents which have a long 'life span', such as passports, which are likely to remain current and so there is greater potential for detriment.

40. LPVL received a complaint from a customer in April 2017 concerning fraudulent applications made in his name shortly after using LPVL's services, including fraudulent credit applications which had adversely affected his credit rating. Whilst LPVL was unable to conclusively link the incident to this breach it is demonstrative of the risks posed to individuals whose data is compromised in a contravention of this type.

41. The Commissioner considers that the damage and/or distress described above was likely to arise as a consequence of the kind of contravention. In other words, the Commissioner's view is that there was a significant and weighty chance that a contravention of the kind described would have such consequences.

42. The Commissioner also considers that such damage and/or distress was likely to be substantial, having regard to the number of affected individuals and the broad nature of the personal data involved. In the circumstances, the likely damage or distress was certainly more than trivial. When forming this view the Commissioner has also paid due regard to the prolonged duration of exposure of the personal data involved.

43. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

Deliberate or negligent contraventions

44. The Commissioner has considered whether the contraventions identified above were deliberate. In the Commissioner's view, this means that LPVL's actions which constituted those contraventions were deliberate actions (even if LPVL did not actually intend thereby to contravene the DPA).

45. The Commissioner considers that in this case LPVL did not deliberately contravene the DPA in that sense.

46. The Commissioner has gone on to consider whether the contraventions identified above were negligent. First, she has considered whether LPVL ought reasonably to have known that there was a risk that these contraventions would occur. She is satisfied that this condition is met, given that LPVL was routinely used to handling large volumes of confidential and personal data relating to tenants (and to a lesser degree landlords). Therefore, LPVL should have been aware that such information must be kept secure and handled appropriately.

47. LPVL stated that its intention had always been to implement password protection to the FTP server, which would suggest to the Commissioner that LVPL had some awareness that such personal data should have been kept secure.

48. Indeed LPVL was a registered data controller with a data protection policy in place, who was aware of and preparing for GDPR when the breach was reported. As such the Commissioner is satisfied that LPVL was aware of its obligations to maintain sufficient technical and organisational measures to protect personal data.

49. In the circumstances LPVL ought reasonably to have known that the files containing tenant's personal data would be vulnerable to a security breach in the absence of appropriate security measures.

50. The ICO has had longstanding guidance available prior to the incident in the form of the 'Data Sharing Code of Practice' and 'A practical guide to IT security' which included technical and organisational security considerations around the sharing of data and keeping IT systems safe and secure. Guidance issued in 2014 (*https://ico.org.uk/media/for-organisations/documents/1042221/protecting -personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf*) highlighted the risks of using FTP for the transfer of personal data. In particular it says: *"Plain FTP should be avoided for transfer of personal data or other confidential information; again because information, including usernames and passwords, is sent unencrypted. Remember too that FTP services can be configured to allow anonymous access which can also be indexed by internet search engines."* This same guidance makes direct reference to anonymous access being a risk. It is considered that LPVL had ample opportunity to be aware of such guidance and to take steps to act upon the advice they contained.

51. The ICO has also published details of regulatory action against other data controllers in respect of similar incidents involving the use of FTP servers to store and transfer personal data (e.g. HCA International Limited - February 2017). LPVL had the opportunity to be aware of these cases and the risks identified by the use of FTP servers to transfer personal data.

52. Second, the Commissioner has considered whether LPVL knew or ought reasonably to have known that those contraventions would be of a kind likely to cause substantial damage or substantial distress. She is satisfied that this condition is met, given that LPVL handled a

significant volume of tenancy related personal data and was aware of nature of the personal data it handled. The types and classifications of personal data transferred by LPVL via FTP are typically of a sort used for individuals to enter into legally binding contracts/tenancy agreements. By their very nature the personal data compromised in this incident can be used to identify individuals, carry out background checks, and conduct credit checks, and if handled maliciously would enable a motivated individual to commit identity and financial fraud. Therefore, it should have been obvious to LPVL that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the affected individuals.

53. Third, the Commissioner has considered whether LPVL failed to take reasonable steps to prevent the contravention. Again, she is satisfied that this condition is met. Reasonable steps in these circumstances would have included:

- Using a secure method to transfer large quantities of personal data to its partner organisation;
- Implementation of access authentication controls/restrictions to ensure personal data could not be accessed by others unless authorised;
- Monitoring of access logs, penetration testing and setting alerts for downloads from the FTP server, to enable early detection and containment of a breach;
- Provision of adequate and timely training, policies or guidance to staff in relation to FTP setup, and information handling and security.

54. LPVL failed to take any of those steps. The Commissioner considers that there was no good reason for that failure.

55. The Commissioner is therefore satisfied that condition (c) from section 55A (1) DPA is met.

The Commissioner's decision to impose a monetary penalty

56. For the reasons explained above the Commissioner is satisfied that the conditions from section 55A(1) DPA have been met in this caseeShe is also satisfied that section 55A(3) and the procedural rights under section 55B have been complied withe

57. The latter has included issuing a Notice of Intent dated 11 June 2019 in which the Commissioner set out her preliminary thinking.

58. The Commissioner is accordingly entitled to issue a monetary penalty in this case.

59. The Commissioner has received representations in response to the Notice of Intent dated 2 July 2019 and has taken these into account when making her final determinationeThe representations do not dispute the contravention itself; more they highlight substantial remedial action and investment in LPVL's IT systems post-breach which the Commissioner has already taken into consideration when issuing her Notice of Intent (see mitigating factors at paragraph 61 below)e In any event the Commissioner's view is that any such security should already have been in place at the time of the contravention. LVPL also point to the financial impact of the penalty on the company, however this is not borne out by the information available to the Commissioner, and LPVL did not provide any evidence in support of this assertion.

60. The Commissioner has taken into account the following **aggravating features** of this casee

- LPVL's delay in reporting the breach to the ICO – the breach was reported only after LPVL was contacted by the attacker in October 2017;
- The longevity of the data was such that it could potentially be live and usable data for a significant time after the breach (for example 10 years in the case of passports);
- Failure to notify affected data subjects who have been unable to take steps to protect themselves against identity and financial fraud;
- The Commissioner has also noted LPVL's lack of policies in regards to retention of data.

61. The Commissioner has also taken into account the following **mitigating features** of this case:

- Since 2016 and throughout 2017, LPVL has made significant investment in improving its information systems, including cyber security - it was during this review that the vulnerability was detected. LPVL took immediate remedial action as soon as the vulnerability was identified.

62. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data.

The amount of the penalty

63. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£80,000** (**eighty**

thousand pounds).

Conclusion

64. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **15 August 2019** at the latest. The monetary 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.

65. If the Commissioner receives full payment of the monetary penalty by **14 August 2019** the Commissioner will reduce the monetary penalty by 20% to **£64,000 (Sixty four thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

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

a) the imposition of the monetary penalty and/or;

b) the amount of the penalty specified in the monetary penalty notice.

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

68. Information about appeals is set out in Annex 1.

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

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

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

70. the period for appealing against the monetary penalty and any In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary 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.

Dated the 17th day of July 2019

Signed [redacted]

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

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary 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 she ought to have exercised her 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

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:-

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 monetary 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 (Information Rights) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).