INDEPENDENT REVIEW

By R.J.B Fowler QC of Commerce Commission
Information Security Incident

R.J.B Fowler QC
email@richardfowler.co.nz

Introduction

1. This review is produced pursuant to a Terms of Reference directed to me dated 25 October 2019. A copy of the Terms of Reference is attached as Appendix 1.

2. The review was commissioned following an incident on [redacted] when a contractor who was holding information obtained or generated by the Commission, was burgled and various items were stolen from the contractor's home. Items of computer equipment relevant to this review were stolen.

3. [redacted]

4. The burglary and theft were reported to the Police [redacted], but thus far none of the stolen goods have been recovered and no arrests made.

5. There is no absolute certainty as to the exact nature and content of the electronic material that has been stolen, or would be available to unauthorised persons accessing the stolen items. But it is very clear that it includes a significant amount of confidential material and on a worst case estimate made in the days after the thefts [redacted]

The review process

6. An index and a full repository of potentially relevant documents was made available to the review. A copy of the index is attached as Appendix 2. Interviews were conducted with the contractor concerned and with the Commission staff listed in Appendix 3.

The functions of the Commission and the generation of confidential information

7. The Commission has a range of functions under several statutes. However, the functions relevant to the issues in this review are as follows:

   7.1. Investigation of potential breaches of the Commerce Act 1986, the Fair Trading Act 1986 and the Credit Contract and Consumer Finance Act 2003;

   7.2. The conduct of competition studies under Part 3A of the Commerce Act;

   7.3. Determining applications for clearance or authorisation of mergers or restrictive trade practices under Part 5 of the Commerce Act;

   7.4. Regulation of industries under Part 4 of the Commerce Act;

   7.5. Industry specific regulation of telecommunications services under the Telecommunications Act 2001 and of aspects of the dairy industry under the Dairy Industry Re-structuring Act 2001;

   7.6. Investigation of potential breaches of industry specific regulation and / or regulations under Part 4 of the Commerce Act.

8. It is self-evident that the above functions extend well beyond court proceedings (both civil and criminal) and include studies, administrative determinations, monitoring functions and numerous investigative functions.

9. It follows that a wide and complex range of often confidential information is collected, most of it not in the public domain. The nature of that confidential information typically held by the Commission covers:

   9.1. Commercially sensitive information, such as business plans and the strategic intentions of companies, forecasts, trade secrets and financial information;

   9.2. Market sensitive information, being information not known to the public that may affect the value of shares in listed companies;

   9.3. Information from confidential sources including informants and whistle-blowers;

   9.4. Legally privileged information, including interviews with witnesses for the purposes of litigation;

   9.5. Personal information relating to individuals.

The contractor's role

10. The work of the Commission described above frequently requires information services. The contractor who was the victim of the burglary and theft provided such an information service to the Commission.

11. While some information services are provided internally, the volume and cost, together with efficiency factors relating to the unpredictable demand, have compelled the Commission to engage external or out-sourced service providers on contract as demand required.

12. The Commission's relationship with the particular contractor here is the subject of a specific ground of review which will be addressed later. From this point on I will refer to that contractor as "C", and that label will include any associated entity which C owned or operated. For the moment it is only required to observe that C had an excellent reputation within the Commission over several generational cohorts of staff for the quality of the work produced, and it seems that C became very much the first choice, or preferred external contractor for that particular information service.

Post burglary steps taken by the Commission

13. Before turning to the particular matters to be reviewed and on which findings are sought, the triage steps taken by the Commission immediately after being advised of the burglary and theft should be briefly traversed – if only by reason of any potential relevance to future risk.

14. The Commission was informed by C of the thefts on [redacted]. A senior legal staff member of the Commission spoke with the contractor at length both that day and again on [redacted] to ascertain with as much precision as possible C's recollections of the material on the stolen computer equipment.

15. Thereafter it seems that there was a comprehensive effort by Commission staff to match that information with the Commission's own records in order to identify the information that may well be accessible on the stolen computer equipment.

16. The Commission then began the process of advising affected parties of the potential disclosure of the confidential electronic material.

17. Simultaneously the Commission issued a public media statement about the issue.

18. The Commission also took the following steps:

    18.1. It engaged with the New Zealand Police attempting to track and secure the stolen material;

    18.2. It issued a notice under s.100 of the Commerce Act forbidding disclosure of information obtained as a result of the theft;

    18.3. It reported the incident to a number of Government agencies, including MBIE, CERT NZ, the Government Chief Digital Officer and the Office of the Privacy Commissioner;

    18.4. It urgently sought and obtained an interim injunction from the High Court against unknown defendants in an effort to further safeguard the interests of affected parties. (The utility of such an injunction is to provide a ready means to prevent or punish unlawful disclosure by serving copies of such orders in quarters where it is feared such disclosure may occur.)

    18.5. It put arrangements in place to ensure that all services of the type at issue were in the meantime brought back in-house;

    18.6. And of course it commissioned this review.

19. Although it is not central to my findings, for what it is worth I struggle to think of anything else that the Commission could have done once it became aware of the thefts on [redacted]. The Commission treated the incident with the utmost seriousness, and moved swiftly and efficiently to minimise any possible damage.

20. My detailed findings are attached as Appendix 4. Necessarily a great deal of the content of that traverses details of the service provider and theft that were suppressed from publication by the High Court on 9 October 2019. I include that content in my report to the Commission, but do not envisage its wider dissemination on the basis of the current High Court orders.

21. I turn now to set out a summary of my findings.

Summary of Findings

22. Although formal contracts were eventually executed, it was unacceptable for the Commission to have allowed the contractor to have provided services for [redacted] to 2009 before being required to enter a formal written contract recording the contractor's confidentiality and security obligations.

23. By 2009 the contractor was clearly under contractual obligations with regard to information security, retention and disposal of confidential material that had been both received by the contractor and further records created by the contractor.

24. It is equally clear that the contractor understood these obligations both at the time and subsequently.

25. The contractor was plainly in breach of those obligations.

26. For the type of arrangement the particular contractor had with the Commission, a certification system may have been effective to have either triggered compliance by the contractor, or to have revealed the breach. The absence of such a certification system was regrettable on the part of the Commission.

27. In addition an audit system might have been similarly effective, although that is less clear on account of the apparent difficulties involved in phsyically accessing a third-party's computer system without compromising other users' (and the contractors own information).

28. Going forward, the Commission needs to confront the choices of how best to mitigate the type of risk at issue here. This probably involves choices that are best made by management.

29. Given the acute sensitivity of much of the work of the Commission and therefore the confidential information it holds, the Commission should consider assuming more direct control of information services, including through any new opportunities that technology will allow.

30. In the period following the incident the Commission treated the situation with the utmost seriousness and implemented a swift and efficient response to minimise any possible damage.

Dated: 13 December 2019

.....

R.J.B. Fowler QC

Appendix 1

COMMERCE COMMISSION NEW ZEALAND
Te Komihana Tauhokohoko

Independent review of information security incident

Terms of Reference

Background

1. An independent contractor to the Commerce Commission (the **Commission**) was the victim of a burglary, in which computer equipment was stolen which contained Commission information (the **information**). The loss of the information through the burglary is referred to here as the **information security incident** or the **incident**.

2. The information was primarily comprised of [redacted]

3. At the time of the burglary some of the information was already in the public domain and non-confidential.

4. Some of the information was confidential to the Commission and/or to third parties. This confidential information included commercially sensitive information, as well some personal information.

5. Police were notified of the burglary by the contractor and steps were immediately taken, and continue to be taken, to locate and recover the computer equipment. The Commission has liaised closely with the contractor, the Police and affected third parties and has taken steps to help protect the confidentiality of the information. The Police investigation is ongoing.

6. The Commission had a longstanding and continuous relationship with the contractor [redacted]. Obligations as to information security had been the subject of correspondence and documentation between the contractor and the Commission during the relationship. The most recent contract for services commenced on 23 February 2018 and included obligations to deliver the services with due care, skill and diligence, to keep records safe, to securely manage and destroy records following completion of the instruction, and to have in place adequate security measures to safeguard confidential information.

Objective of the review

7. The Commission is entrusted with confidential information in the course of its operations, and effective, secure information handling is important to public confidence in the Commission.

8. The objectives of the review are to:

   8.1 Consider the relationship between the contractor and the Commission, with a focus on the nature and scope of services, protection of confidentiality, and information security requirements and their implementation; and

   8.2 Identify any steps the Commission can take to mitigate the risk of a similar incident occurring again.

Appointment

9. The Board of the Commission appoints Mr Richard Fowler QC of Wellington, to conduct an independent review of the incident.

Scope of the review

10. Mr Fowler QC will review and make findings on, and report to the Board regarding, the circumstances surrounding the information security incident, in particular:

   10.1 The Commission's relationship with the contractor over time including:

      10.1.1 The nature and scope of services requested from, and provided to the Commission by, the contractor during the relationship;

      10.1.2 Relevant contractual terms and conditions applying during the relationship;

      10.1.3 The nature and scope of confidentiality and information security requirements applying to the contractor during the relationship;

      10.1.4 The nature of engagement with the contractor by Commission staff during the relationship, including instructions, discussions, documentation and/or correspondence relevant to the provision of services, contract and relationship management, and the communication and implementation of contractual, confidentiality and information security requirements;

   10.2 Any recommended steps the Commission could take in relation to the matters reviewed to mitigate the risk of a similar incident occurring again; and

   10.3 Any other matter Mr Fowler QC considers (in consultation with the Board) to be relevant to provide a complete report to the Board on the circumstances surrounding the incident.

Process

11. Mr Fowler QC will promptly commence review of the relevant material and will interview relevant personnel (refer [20]-[21] below).

12. The Commission and its personnel will provide all reasonable assistance required by Mr Fowler QC towards completion of this review.

13. Mr Fowler QC will produce a draft report to the Board and, in consultation with the Board, to any materially affected Commission employee, on or before 2 December 2019. Mr Fowler QC will consider and incorporate relevant comments as appropriate. The final report is due on or before 16 December 2019.

14. Mr Fowler QC will, if asked by the Board, produce a summary of his final report as per [22] below.

15. Mr Fowler QC will comply with the obligations of natural justice as necessary. He will anonymise any references to individuals except where reference is necessary to understand the report.

Confidentiality of review records

16. Mr Fowler QC acknowledges that all review-related material is received in confidence and in the expectation that such confidence shall be strictly respected. He agrees to hold securely all confidential information received during the review, and to return it to the Commission within 20 working days of completion of the final report, unless otherwise agreed by the Commission.

17. Mr Fowler QC agrees not to make any public comment in relation to the review, other than to confirm his appointment, unless agreed by the Commission.

18. Mr Fowler QC acknowledges that the Official Information Act 1982 applies to all information held by him on behalf of the Commission, and will assist the Commission where requested to do so in responding to any request under that Act.

Relevant materials and interviews

19. The Commission will make available all relevant information and any of its members, employees or contractors to provide information to and/or to be interviewed by Mr Fowler QC.

20. Mr Fowler QC may interview relevant Commission personnel, including but not limited to:

    20.1 The Chief Executive;

    20.2 The General Managers of each Branch;

    20.3 The relevant contract manager and other staff involved in commissioning the contactor's services;

    20.4 Any other Commission employee responsible for information security and/or the contracting of third party services involving receipt of Commission information;

    20.5 The contractor concerned; and

    20.6 Any other person who may provide information relevant to the matters set out in paragraph [10] above.

21. To the extent practicable, Mr Fowler QC will consult with the Commission and KPMG in respect to that firm's broader review of the processes of the Commission regarding

information handling, but noting that this review will be completed before the broader KPMG review.

Publication

22. The Board may discuss the review findings publicly and may decide to release the final report or a summary of it (subject to ensuring anonymity, privacy, protection of confidential information, natural justice obligations and suppression orders made by the High Court on 15 October 2019).

Timetable and Terms of Reference

23. The Board may amend the timetable for provision of the report and may amend these terms of reference in consultation with Mr Fowler QC.

Dated: 25 October 2019

Anna Rawlings

Chair

Appendix 3

List of Commission staff interviewed

- Catherine Butterworth – Principal Investigator (Consumer)
- Barrie Sutton – Principal Investigator (Cartels)
- Brigid Hewitt – Operations & Legal Support Team Leader
- Nick Russ – General Manager (Regulation)
- Ben Hamlin – Deputy General Counsel (Competition)
- Antonia Horrocks – General Manager (Competition & Consumer)
- Bill Moses – Chief Information Officer
- Geoff Williamson – General Manager (Operational Support)
- Adrienne Meikle – Chief Executive

APPENDIX 4

A profile of the relationship with the Contractor

1. This section of the review is a profile of the historical relationship between C and the Commission, as relevant to the confidentiality issues for the purposes of this review.

2. C's first contractual involvement with the Commission appears to date from as early as [redacted] – at that stage evidently on an ad hoc basis. [redacted] On 12 July 2005 the work flow had become regular enough that C sent the Commission an email attaching "My Pricelist and Terms of Services FYI", but unfortunately that attachment cannot now be found.

3. Certainly by the end of 2005 C was regularly [redacted] Indeed by 18 December 2005 C was [redacted] while travelling overseas.

4. By April 2006 it is clear that the relationship was flourishing, and on 11 April 2006 a senior Commission staff member recommended C to external counsel for use as a [redacted] on the basis that C "is highly recommended by the [redacted]".

5. By this stage (mid-2006) the modus operandi that had been adopted was for the Commission to [redacted]

6. At this point the issue of recording formal confidentiality obligations on C's part explicitly arose for the first time. On 29 May 2006 there was an email internal exchange regarding the use of out-sourced [redacted] and the following observation was made:

> *"Internally we do not have the capability to* [redacted]

7. In the course of that exchange the issue arose of ensuring that any external agency or person doing [redacted] agreed to maintain confidentiality. It seems that further enquiry was made, and in the case of C it became evident that although both C and the Commission were quite clear that there was an existing implicit confidentiality obligation on C, there was no discrete confidentiality agreement. There was also some discussion as to whether this should be addressed through a stand-alone confidentiality agreement, or whether such obligations should form part of a comprehensive contract covering all terms.

8. Thereafter it seems that the issue of explicitly recording confidentiality obligations with C was parked – at least for a period. C continued providing [redacted] through the remainder of 2006, 2007 and into 2008 without that issue arising again. However, it should be noted that during that period:

8.1. There are at least three instances where Commission staff had apparently mislaid [redacted] and then asked C if C still had [redacted] on C's system some two to three months later. C was able to helpfully oblige by providing [redacted] which therefore must have been undeleted on C's system.

8.2. By mid-2007 at least some [redacted] were being sent to C by email.

9. The issue of an explicit confidentiality agreement re-emerged on 8 July 2008. It is not clear what triggered the enquiry, but the exchange proceeded as follows. A Commission staff member emailed C thus:

> *"Presumably you will have a signed confidentiality agreement when you first started [redacted] Do you recall doing so and if so when and who were you dealing with here? We don't have a copy on our floor and would like to track it down."*

10. C replied that that question had been asked before and added:

> *"I haven't ever signed one. Happy to of course."*

11. The next step in progressing a confidentiality agreement occurred on 10 February 2009 when C was sent a draft Confidentiality Agreement. The covering email is important because:

11.1. It states that it is intended to cover C's work *"globally across the Commerce Commission";*

11.2. It asks C to review the draft and to get advice;

11.3. It states:

> *"As you would be aware from the recent encryption process, we are tightening up on security and there is a requirement in the agreement that [redacted] you hold are destroyed (including deleted) within five days of written confirmation of receipt from us and this includes that all previous [redacted] are destroyed within five working days of the commencement date of the agreement."*

11.4. It acknowledges that C sometimes uses previous [redacted] for reference, and says that in this situation the Commission would send C a copy of the former [redacted] and ask that it be destroyed within five days of the new [redacted] being received;

11.5. It sets out a form of acknowledgement that Commission staff will send C confirming [redacted] is lodged in the Commission's records and that C's copy is no longer required and should be expunged from C's records.

12. Evidently C did take advice on the agreement and raised a slight query over the need for the disclaimer clause, which was answered. Following that C indicated a

willingness to sign the agreement which both parties did and the agreement, which is in the form of a deed, is dated 2 March 2009. The document is only directed to confidentiality and is described as "Confidentiality Deed". The precise terms are referred to in more detail later in this review, but for the moment it is worth noting that it defines "Confidential Information", explicitly sets out a Duty of Confidentiality at Clause 3, imposes Security Obligations at Clause 4 and a Destruction Regime (as foreshadowed in the covering email mentioned above) at Clause 9. There is no reference to a duration term.

13. Following completion of the agreement a Commission staff member emailed C asking that C now delete or destroy all historic copies of [redacted] already sent, and C replied acknowledging that that would be done.

14. C continued to provide [redacted] services on request. On 9 February 2010 C adjusted the contractual rate and sent a fee schedule described as "Terms of Service" that addresses such matters as disbursements and cancellations.

15. By 2010 the dominating technology appears to have become the use of USB Sticks ("Ironkey") with an email communication from the Commission of the applicable password. A Commission "Task List" from March 2010 covering a number of Commission activities includes a sub-section on [redacted] C is described there as "the main [redacted]". The task list goes on to state that all [redacted] were to be sent on encrypted USB sticks that were kept in a particular place at the Commission. Copies sent to C were to be recorded in a particular identified document located in a particular part of the Commission's then intranet. The task list continued that each USB had its own password and that C already had a record of these.

16. On 30 March 2010 C advised the Commission of an ability to PDF [redacted].

17. On 14 March 2011 a further "Confidentiality Deed" was signed. Its provenance is unclear. It uses different terminology from the 2 March 2009 deed, and the confidentiality terms are worded differently.

18. The document copy in the Commission's records also appears to be incomplete.

19. Of the provisions that are available, while the wording is different from the 2009 document, those differences do not appear to be material.

20. On 9 May 2011 C [redacted]

21. Through 2011 the relationship between C and Commission continued to flourish. C's work product was described as "excellent", and C was recommended to and utilised by further arms of the Commission. Nonetheless, the confidentiality issue did arise occasionally and its importance emphasised by Commission investigators.

22. The Commission's IT systems staff set up new [redacted] software on 4 October 2011, although that did not change the use of encrypted USB memory sticks.

23. On 16 November 2011 a senior Commission staff member requested C to [redacted] The staff member had not dealt with C before. However, at the end of that enquiry the staff member also asked if C had any kind of services contract and if not, one would be sent. The staff member added:

> *"This just covers off things like confidentiality, etc of the material [redacted]"*

24. C replied in the following terms:

> *"I signed something a while ago regarding confidentiality, although I can't remember if it was specifically for that job or an indefinite one. I'm happy to sign another one,"*

25. A one page document entitled "Confidentiality Undertaking" was then sent to C who signed it on 24 November 2011 and returned it. The terms of that document are different from either the 2009 or 2011 documents. The relevant terms will be examined later along with whether the differences are material.

26. Normal [redacted] service by C continued. On 1 December 2011 C raised a concern about [redacted] possibly being mislaid in the post, but that turned out to be a false alarm.

27. On 12 September 2012 C was set up with access to the Commission's Extranet. Utilising a password, the objective was for C to download [redacted] directly. However that proved unsuccessful because C's Vodem could not handle the size of the files. The previous system was therefore continued for the time being utilising a USB stick.

28. In 2013 C enquired about utilising a colleague to assist with the turnaround time. In making the request C said:

> *"I am aware of the sensitivity and confidentiality of the content and would stress that to [redacted] and [redacted] would not have access to the website if you are not comfortable with that."*

29. The Commission approved that request and in doing so pointed out that Clause 3.2 of C's confidentiality deed covers "affiliates" provided they agreed to keep information confidential in accordance with the deed. The Confidentiality Deed attached to that reply was the deed dated 2009, not the 2011 one.

30. On 10 April 2014 a senior Commission investigator forwarding [redacted] on the extranet for [redacted] observed that documents supplied were done so under the existing confidentiality arrangements between C and the Commission.

31. On 29 May 2014 a senior Commission staff member sent C [redacted]

32. On 15 October 2014 C advised of an inability to access an extranet file and requested that it be emailed instead. While that drew a positive response from the Commission, the staff member concerned sought confirmation that C was still under a current confidentiality agreement. On the following day the staff member forwarded a copy

of the 2 March 2009 deed, but stated uncertainty if C had signed an updated document since then, and that the HR team had suggested C sign a newer updated version which would be arranged.

33. C indicated a willingness to do that.

34. On 26 February 2015 it is recorded that there was now a "shared network drive" used to share [redacted] uploaded by the Commission which C could download.

35. On 22 September 2015 a Commission memorandum on [redacted] describes the then current process for provision of [redacted] as providing the following options:

35.1. Extranet access making them available for download;
35.2. Copy sent on to a secure USB Ironkey device;
35.3. File can be attached to email if small enough.

36. On 4 November 2015 a Commission senior investigator requested C not to throw away [redacted] once C had finished with them.

37. The last sequence in which confidentiality obligations with C came under scrutiny appears to have been between 26 February 2018 and 25 May 2018. In that period a senior Commission staff member deployed to review job quotes and commissioning enquired of C whether C had signed a confidentiality agreement "recently". The staff member adds:

> *"I don't think you have in my time here but you may have signed a "lifetime" one before that."*

38. C replied that one had been signed a few years ago but was happy to sign another if need be. The staff member then forwarded a "Contract for Services" which was then signed and returned. This document is expressed as an agreement, not a deed, and is dated 2 March 2018. Schedule 2 sets out information management obligations at clause 5, confidential information security obligations at clause 13, and defines 'confidential information' at clause 17.

39. On 25 May 2018 the system was further refined with the first appearance of Box.Com as a means of uploading and sharing [redacted] C was instructed:

> *"You are required to add a password, you may get a few registration questions pop up which you can choose to skip and possibly a security message.... then select download."*

C's position

40. On interview C explained that the relationship had grown rather organically from its [redacted] beginnings with the work being received on an ad hoc basis. Information security and confidentiality was a "given" for C on account of the subject matter and other similar contracting work that C was doing and continues to do.

41. C states [redacted] were always deleted [redacted] However C's deletion of [redacted] was much more random. C had

developed a pattern whereby at the end of each year a major deletion exercise would be undertaken, but C thought that by reason of pressure of work that had not happened at the end of 2018. It was because of this that initially C told the Commission that possibly [redacted] may have been on one of the stolen devices. However, on further reflection C now thinks that it is highly unlikely that they go that far back [redacted]

42. C acknowledged the contents of the four documents recording confidentiality and information security obligations but, [redacted] In hindsight C acknowledges that this was careless, particularly as C had been burgled on an earlier occasion in 2018 – although on that occasion the devices were not at the property that was burgled.

43. When C had used a colleague to assist with the work flows, C was aware that that colleague regularly deleted material. The colleague did not have access to the Commission's Extranet.

44. C's contact and engagement with Commission staff was cordial but occasional. This would involve meeting staff [redacted] on a fairly infrequent basis, and occasionally dropping something off at the Commission's offices when C was in Wellington. Very few of the Commission staff interviewed for this review had met or spoken to C, and for a number of those that had, it was barely once or twice.

Commission information security protocols

45. It is necessary to identify the provisions of any Commission information security protocols relevant to this review.

46. Whatever earlier regimes or policies might have provided, the most relevant Commission documents would appear to have been first approved by the Commission's Senior Leadership Team on 29 April 2013. The highest level document setting Commission Policy for information and records management is *"Commerce Commission Information and Records Management Policy: Managing Commission Information Securely" approved* by the Senior Leadership Team on that date. That policy deals with a good deal more than just security issues, but in terms of those matters states the following principles:

> *"Records must be managed securely and systematically across both record keeping and business systems;*
>
> *Records retention and disposal must be authorised."*

47. Indeed that document records that as a public agency the Commission has an obligation to follow the principles of the Security in the Government Sector Guidelines.

48. The policy explicitly extends to contractors.

49. Other relevant policies are:

"A record keeping programme with defined risk management procedures, resources and allocated responsibilities is in place, and monitored."

"Deletion or transfer of records occurs regularly, and is monitored and reviewed."

50. The document goes on to attribute information and record management roles down through the tiers of staff.

51. The second document approved on the same date is "*Commerce Commission Information Securities Procedures*" which states it must be read in conjunction with (inter alia) the above described Information and Records Management Policy.

52. It is expressed at the very beginning as providing a clear set of information security procedures "for all staff and contractors" to confidentially secure, protect and release Commission information. The document covers many logical and sensible security measures, most of which would be unremarkable within organisations that handle sensitive material. Despite the inclusion of a reference to contractors, there is no specific provision in this document that addresses the interface with external [redacted] services or deletion or destruction of material in the possession of contractors after they have finished working on them.

53. The Commission also had available over this period some standard form agreements or terms that could be injected into agreements. These consisted of a standalone "Commerce Commission Short Form Consultancy Agreement" and a Government Model Contract term for confidential information – one version applicable to services and the other to goods.

54. Turning to security reviews, in May 2014 KPMG completed an IT Security Review for the Commission. This was the first such security review the Commission had undertaken. In its key findings KPMG concluded:

"The review has identified that the security in place is not in line with the risks posed. A wide range of issues were identified during the assessment, some of which are relatively significant.

The nature and volume of issues identified however, is typical of what we have observed when we have undertaken a security review for the first time for other organisations of a similar size and complexity."

55. A number of issues were identified, one of which was:

[redacted]

56. Of course it needs to be remembered that that observation was being made in respect of the Commission's own [redacted]

57. A section of the KPMG report does address external security and there are a number of detailed findings and recommendations, although again there is nothing that is specifically relevant to the security of documents [redacted] still held on a contractor's device.

58. Interestingly, on 7 October 2014 [redacted] made a request to the Commerce Commission under the Official Information Act 1982 for information regarding the Commission's protection of [redacted] confidential information. That included a request for information as to how the Commission shared confidential information with third parties.

59. That request was answered on 21 November 2014. The response included the following passage:

> *"When we send out confidential information in electronic format, this can be done using email, the Extranet facility or specifically created data rooms. If we send information out in a physical format such as paper, disk, Iron Key Flash drives or key coded external hard drives, these are couriered in a sealed package.[2] The method we use to send information externally depends on the type of information, the reason it is being sent, and the person or people being sent the information."*

60. The Footnote stated:

> *"Security codes for the Iron Key or key coded external hard drive facilities are emailed to the recipient separately."*

61. In another part of the response the following is said, albeit evidently directed to staff working arrangements:

> *"Storage devices such as Iron Key flash drives and more recently key coded external hard drives are used to take electronic copies of information outside of secure premises. The Commission also operates a secure remote location facility for staff, which limits the need to copy information onto these types of devices. Staff can use this facility to access work related information on their home computers, smart phones and IPads/Tablets."*

62. More germane to contractors, the next paragraph continues:

> *"... When confidential information is provided to an authorised third person on digital storage device or paper it is to be sent via courier in a sealed envelope or package. All external authorised persons other than the Commission's lawyers are either subject to a Contract for Service (with confidentiality terms) or a specific Confidentiality Agreement."*

63. In 2017 Awa Information Security conducted a further review of the Commission security systems. Although similar to the KPMG 2014 review, the terms of reference and focus were primarily directed to internal systems, and not external information security. Nonetheless there were a number of security enhancements that flowed from those two reviews, such as staff use of Microsoft surface devices with password protection and the ability to remotely delete material.

64. The *"Commerce Commission Information Security Procedures"* document was updated on 23 July 2015. However, the particular provisions relating to security measures and reference to contractors were not materially changed and no fresh provisions were added that are of particular relevance to this review.

65. On 22 September 2015 the Commission produced a document of which the "owner" is described as Competition Investigations, Wellington. It sets out the [redacted] process when that part of the Commission [redacted]

[redacted]

66. In an attached table [redacted] process is set out in a series of required steps. There is no reference to deletion or destruction by [redacted] contractor or for staff to check that has occurred.

67. On 3 May 2016 an internal document was created by the Commission setting out the Commission's requirements for [redacted] The idea appears to have been to draw all the Commission's functional and non-functional business requirements on this topic together in one location. The previous "Summation" [redacted] software was regarded as inefficient and poorly performing in high volume cases. Most of the document addresses [redacted] and although there is occasional reference to the interface with external parties, there is nothing that bears directly on the expectations concerning the external party or what happens at the completion of the interaction.

68. The *"Commerce Commission Information Security Guidelines and Procedures"* document was updated by the Senior Leadership Team on 13 April 2018 but none of the updating changes are material to this review.

Confidentiality Agreements between Commission and Contractor

69. As foreshadowed earlier, this part of the review examines the detailed terms of the formal confidentiality obligations recorded between C and the Commission.

70. Starting with the confidentiality deed dated 2 March 2009, this document is directed to confidentiality obligations and does not cover C's broader contractual arrangements. It describes C as "the Consultant".

71. As one would expect, "confidential information" is broadly defined. There could be no question but that information constituted in the material [redacted] sent to C and [redacted] provided back to the Commission would fall within that definition.

72. Clause 3 sets out the duty of confidentiality. The relevant provisions are as follows:

> *"3.1: The consultant acknowledges and agrees that:*
>
> *(a) The consultant shall keep the confidential information strictly confidential and shall not, either during or after the performance of the services, use or disclose any confidential information other than in the proper performance of the services;*

(b) The consultant shall not directly or indirectly disclose, distribute or permit to be disclosed or distributed any confidential information in whole or in part to any person, except in accordance with clause 3.2;

3.2: Notwithstanding clause 3.1, the consultant may disclose confidential information to those of its affiliates who need to have access to the confidential information in order to enable the consultant to provide the services, provided that such affiliates have agreed to keep the information strictly confidential on terms equivalent to those set out in this deed"

73. Clause 4 addressed security. It provides (inter alia):

"4.1: The consultant must, at its expense:

(a) Institute effective security measures to prevent unauthorised access to or use of the confidential information;

(b) Keep the confidential information under its control and stored in a manner that only it and its authorised directors, officers, employees, agents, consultants, professional advisers and contractors may access it."

Clauses 4.1(c),(d) and (e) address steps that must be taken if the consultant becomes aware of any suspected or actual disclosure or breach of the agreement.

74. Clause 6 requires the consultant to indemnify the Commission against liability arising from any breach.

75. Clause 9 specifically addresses destruction of copies. It provides as follows:

"9.1: Upon written acknowledgement by the Commission of its receipt of a [redacted] *the consultant shall destroy all confidential information in its possession which relates to* [redacted] *unless otherwise directed by the Commission.*

As soon as practicable after receipt of an acknowledgement of receipt pursuant to clause 9.1, and in any event within five working days, the consultant must:

(a) return or destroy all copies of the confidential information which relates to [redacted] *in the possession or control of the consultant or any person to whom the consultant has provided confidential information; and*

(b) certify in writing to the Commission that the consultant has made due enquiries and is satisfied that all the confidential information which relates to [redacted] *in the possession or control of the consultant or any person to whom the consultant has provided confidential information has been returned or destroyed and that no confidential information which relates to*

[redacted] *has been retained by or on behalf of any such person."*

76. This confidentiality deed is silent as to duration term.

77. The second document is dated 14 March 2011 and is also described as a confidentiality deed. The version held by the Commission and provided for this review appears to be incomplete and stops at clause 5. As its title suggests, it appears to only address confidentiality obligations as per the 2009 document.

78. However, although similar, the provisions of this document are nonetheless different from the 2009 document, and in more ways than just minor detail. For example, the duty of confidentiality is expressed in a completely different way. Further, on account of the fact that it appears to be a partial document, it is unclear as to whether it also went on to address issues of security or destruction of copies as the 2009 document did at clauses 4 and 9 respectively.

79. If this second document marked the end of the document trail, some sort of comparison and analysis of those differences from the 2009 document might well be necessary, along with an attempt to obtain and examine the complete document. However, that is not the case because there are subsequent documents.

80. Barely 10 days after signing the 2011 confidentiality deed, C signed a "Confidentiality Undertaking" on 24 November 2011. This one page document is exiguous to say the least, but relevantly provides that C undertakes to:

> *"(1) Acknowledge and agree to preserve the privacy and confidentiality of:*
>
> *(a) the existence of the Commerce Commission's ("the Commission") investigation;*
>
> *(b) the content of any discs and / or* [redacted] *files ("the documents") provided to me by the Commission;.....*
>
> *(4) I will keep secure any of the documents that are provided to me.*
>
> *(5) I will, at the request of the Commission, immediately destroy or return to the Commission all copies of the documents provided, together with all notes or other material (in whatever form) derived from* [redacted] *the documents, and will confirm in writing to the Commission that this has occurred."*

81. On 2 March 2018 the Commission and C signed a "Contract for Services". This document was the fourth and last formal document signed by C and was intended to be a comprehensive contract covering the parties' rights and obligations, rather than just being directed to confidentiality obligations alone. It is evident that a standard or template contract document was being used. It constitutes a coversheet that refers to and attaches two schedules, and the coversheet also functions as the signature page. Schedule 1 contains the contract details and description of services (including the fees), and Schedule 2 contains the standard terms and conditions applicable where services are provided and seems to be an attempt to record all the applicable obligations. Relevant to this review are the following provisions:

"5.1: The supplier must:

(a) Keep and maintain records in accordance with prudent business practice and all applicable laws.....

(c) Keep the records safe.

...

5.5: The supplier must make sure that records provided by the buyer or created for the buyer, are securely managed and securely destroyed on their disposal.

...

13.1 Each party confirms that it has adequate security measures to safeguard the other party's confidential information from unauthorised access or use by third parties, and that it will not use or disclose the other party's confidential information to any person or organisation other than:

(a) to the extent that use or disclosure is necessary....

13.2 Each party will ensure that its personnel:

(a) are aware of the confidentiality obligations in this contract, and

(b) do not use or disclose any of the other party's confidential information except as allowed by this contract."

82. Clause 17 also sets out a definition of "confidential information", and although that definition differs from definitions of that term in the earlier documents, the differences are immaterial vis-à-vis the confidential information at issue here.

83. It would be possible to immerse this review into a finely grained comparison of the differences between the four documents. However, that is unnecessary for the purposes of this review because:

83.1. Common to all of them is an obligation on C to take whatever steps are necessary to keep the confidential information secure while in C's control;

83.2. Common to first, third and fourth (the position is unknown in respect of the second) is an obligation to delete or destroy the confidential information that C was holding after the [redacted] service had been completed.

84. To the extent that there is a detail difference at all, it relates to second of these obligations in that the 2009 and 2018 documents provide for destruction / deletion that is automatic, whereas the confidentiality undertaking of 24 November 2011 appears to require a request from the Commission. However, that difference does not appear to matter because, on the evidence of the exchanges between the Commission and C, it seems quite clear that the Commission had in fact implemented

a generic request for such destruction / deletion: see the emails dated 10 February 2009, and confirmed again after the 2009 document was signed.

Conclusion to this point on written contracts

85. On the basis of the above analysis, in my view it can be safely concluded at this point that C was in breach of C's legal obligations to the Commission in two respects:

85.1. Failing to take adequate steps to [redacted] secure the Commission material on the stolen devices;

85.2. Failing to delete or destroy the confidential information after [redacted] had been completed (save for those that were very recent).

86. The Terms of Reference nonetheless require an examination of whether there was more that reasonably could have been done or could be done to mitigate the risk of a similar incident occurring again.

The Commission's awareness of possible breaches

87. Other than to enquire whether C was utilising [redacted] protection on devices being used, there was probably not a great deal more that the Commission could have done or expected as to the security of access on the devices themselves. A certification process would have been a possibility, but in terms of the historical events there was nothing to put Commission officers on notice that C's security measures were as deficient as they turned out to be.

But the position could be a little different on destruction / deletion. There had been some earlier history of positive responses to requests that were made by Commission staff for replacement or additional [redacted] had been provided some months previously although these occurred prior to the first formal agreement and the subsequent email directions on deletion. There was also the request on 4 November 2015 when C was asked not throw away some [redacted] – although that is more marginal and could be argued both ways.

88. To be fair, there is a natural human element to that that mitigates the point. In those earlier instances C was assisting the Commission in circumstances where [redacted] had been mislaid or lost. It would be remarkably churlish for Commission staff members who had been helpfully provided with missing [redacted] by C, to immediately turn round and reprimand C for the breach of the obligation.

Mitigation of Risk within pre-incident arrangement

89. If the pre-incident arrangements were to continue, there are steps that could be taken by the Commission which would hopefully mitigate the risk of this compromise of security occurring again. Those steps are to require certification by a [redacted] contractor at particular points together with an audit function, and perhaps to grade

the sensitivity of material being considered for external [redacted] Those steps in a little more detail would be:

89.1. Certification as to the security that the contractor is implementing to the contractor's access to [redacted] The precise technological method does not matter and can adapt to the technological evolution. The point is the same: whatever way the contractor attains access, the responsibility would be on the contractor to provide adequate security vis-à-vis [redacted] The Commission could seek certification at times or in ways to be fixed as to the adequacy of that security. Such certification could be a contractual requirement.

89.2. After [redacted] have been provided, the destruction / deletion obligation could also be a matter of certification in the same way at a time to be fixed and for a period subsequent to [redacted] dispatch. There could possibly be a contractual requirement to make such certification part and parcel of the contractor's invoicing.

89.3. Both those steps could be the subject of Commission audit.

89.4. The sensitivity of material being considered for external [redacted] could be graded with the highest level being retained in-house.

90. However, a more fundamental issue must be faced as to whether the pre-incident arrangement itself should be abandoned in order to address the risks at issue. That raises the question of what the alternatives might be.

Tiers of security: the alternatives

91. In descending order of security, from the enquiries made in this review there are broadly four possible tiers of security. They are as follows:

91.1. The [redacted] function could be provided entirely in-house – i.e. [redacted] would be performed entirely on the Commission's premises and by employed staff.

91.2. The [redacted] function could be provided entirely in-house but by external contractors brought onto the Commission's premises.

91.3. The [redacted] function could be provided remotely and by utilising external contractors, but using only dedicated Commission property, such as a Commission laptop.

91.4. The [redacted] function could be provided remotely by external contractors using their own devices – i.e. the pre-incident arrangement.

92. Of course while some of these alternatives might provide better opportunities to mitigate risk, they also have cost and utility trade-offs.

93. The first alternative (bringing the [redacted] function entirely in-house) while carrying the least risk, has some significant potential budgetary and organisational imposts at present. (That "at present" qualification should be noted and is an aspect

to which this review will return.). Senior Commission staff pointed to the budgetary restraints and the difficulties of meeting volume volatility from an organisational point of view with hiring fixed term or temporary employees.

94. The second alternative (bringing the [redacted] function entirely in-house but staffing it with external contractors brought onto the Commission's premises) seems to be one of the two preferences of senior staff that meets a higher level of security but addresses volume volatility, and therefore budgetary and organisational issues.

95. The third alternative (providing the [redacted] function remotely utilising external contractors but using only Commission property) also has some support from senior staff. The security level might be considered to be lower, but the technology now permits a high degree of control over such remote property with an ability to immediately remotely destroy data. The budgetary and organisational impost may be similar or even lower than the second alternative.

96. The fourth alternative (providing the [redacted] function remotely by external contractors using their own devices) was the arrangement up until [redacted] and as per the contract with C. It carries the lowest level of security but the greatest degree of flexibility. If it were to be continued it would need to now be augmented by:

96.1. Some form of certification by the contractor as to [redacted] and then subsequent destruction / deletion; and

96.2. Some form of audit regime.

96.3. And possibly some sort of sensitivity grading filter.

It would be fair to say that Commission staff interviewed for this review did not consider that a continuation of this form of provision of [redacted] services was tenable in the light of what had occurred. Even aside from that there would still be a risk with regard to the anti-virus status and internal network set up at the contractor's home over which the Commission would have no control.

97. Of course it is not the function of this review to intrude on what are properly purely management choices. But it is considered to be within the Terms of Reference to identify alternatives that would mitigate the risk of a similar incident occurring again.

98. The problem with the fourth alternative in my view is that it would always carry an inherent risk that the remote contractor will not meet the security requirements, or that over a period of time and volume driven repetition, lapse. It is questionable whether even the measures referred to above will provide the level of reassurance necessary given the acute sensitivity of much of the information. It is worthy of note that C provided a reliable service and a very high work quality product. There was no reason to suspect C of any form of lapse. Yet, despite there being three or possibly four formal documents recording the two fundamental security obligations at issue here, they simply were not observed.

A temporal factor

99. There is an important issue of timing that now needs to be brought to bear vis-à-vis the alternatives discussed above.

100. With regard to the first alternative (bringing the [redacted] function entirely in-house) the observation was made above that whilst carrying the least risk, at present it has some significant budgetary and organisational imposts. The qualification "at present" becomes important.

101. The acquisition of [redacted] would enable the [redacted] function to be brought entirely in-house. This issue has been explored with the relevant Commission staff and it would seem that the position is as follows:

101.1. [redacted]

101.2.

101.3.

102. There is an irony to the suggestion that in order to achieve the highest tier alternative of security, Cloud security concerns must be disposed of first. But the understanding of this reviewer from the relevant Commission staff is that in fact robust security levels can be attained for Cloud based information storage. What will be required to enable this change will be the verification of that and attribution of some degree of priority.

103. The impact on mitigation of risk and assessment of alternative arrangements is this: even if it takes longer than two years, a migration to [redacted] operated entirely in-house will enable the best level of control of risk and should be economically and organisationally efficient. However, until that migration occurs, one or more of the other three alternatives would need to be utilised.

Conclusions

104. This final part of the review draws the threads together in terms of paragraph 10 of the Terms of Reference.

105. C provided [redacted] services from [redacted] to 2019. [redacted] The services did not extend beyond that. The requests for services were relatively ad hoc. Requests came from a variety of sources.

106. From [redacted] until 2009 there was no formal written confidentiality / information security obligation. This was self-evidently an undesirable gap that ought to have been addressed a long time before it eventually was. Yet between 2009 and 2018

four distinct documents were signed by C that did contain such provisions. At least one can conclude from this phase an evolution of a heightened sensitivity to the need for information security vis-à-vis the contracted service. While the precise terms, formats and document scope varied, in my view nothing turns on that. There is no doubt that C was bound by legal obligations in respect of C's receipt of confidential information from the Commission and the creation of further confidential information (i.e. [redacted]) by C for despatch back to the Commission.

107. The nature of C's engagement with the Commission for the earlier part of that period was sporadic and rather diffuse. For much of the period there was no single point of contact and the very fact that there ended up being four separate documents probably underscores that. Notwithstanding that, there does seem to have been a consistent message to C as to the importance of information protection and security. Whilst it is possible that a more centralised procurement system would have picked up the fact that C was not conforming with the destruction / deletion obligation, or could have sought some form of certification or imposed an audit, C who was otherwise an exemplary contractor in terms of work product, was unusually reckless and, it is suggested, rather unique in not [redacted]

108. Certainly a form of certification, perhaps linked to invoicing, may have been effective in triggering compliance by C, or would have forced C to reveal the breaches. It is to be regretted that that was not done. An audit might have been effective, although that is less clear because, to be sure of that and to have tested the compliance with the obligations that were breached here, there would have had to have been some fairly intrusive requirements that could have raised privacy issues.

109. Going forward, on the evidence available to me, the medium term solution is a migration to [redacted] operated entirely in-house. But that could be two or more years away.

110. During that period the best mitigation options would appear to be the second and / or third alternatives discussed earlier i.e.:

110.1. Moving the [redacted] function entirely in-house but utilising external contractors;

110.2. Allowing the [redacted] to be provided remotely by external contractors but using only dedicated Commission property.

111. The precise arrangements and choices are quintessentially matters of management, and not for this review. Senior staff without exception considered one or both of those arrangements should be preferred and I have seen no reason to differ from that assessment.

112. A continuation of the pre-incident arrangement ([redacted]) is probably not tenable. As traversed at the commencement of this review, the Commission is dealing in confidential information of acute commercial and other sensitivity. The problem with the pre-incident arrangement is that it exposes the Commission to the propensities of external contractors over whom it has only ostensible control through legal contractual mechanisms.

113. Since this review is undertaken by a lawyer I finish with the following observation made by [redacted] that I consider to be apt here:

> "Lawyers think that just because it is in a contract it will happen and are surprised and dismayed when it does not."

114. It is the risk of exactly that failure that can only be properly minimised here by the Commission taking back more control.