

**From:** "Westbrook, Mark (UK - Manchester)" <[REDACTED]>  
**To:** "Gribben, Jonathan" <[REDACTED]>  
**Cc:** "Keating, Lewis (UK - Leeds)" <[REDACTED]>  
**Subject:** RE: Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report  
**Date:** Tue, 8 Nov 2016 14:14:45 +0000  
**Importance:** Normal  
**Inline-Images:** image001.jpg; image002.png; image003.png

---

Hello Jonny,

Apologies for the delay.

Thoughts on the summary are as follows (apart from the key point you already recognise upfront that you have by definition collapsed certain matters / removed some detail that is present in the overall report:

2.1 – Ok, maybe worth calling out in 2.1.3 that this is a theoretical risk and outside of ‘processes’

2.4 – this is true, but the main segregation of duties point we are making is around access to fake a digital signature, rather than access to audit logs. If you can’t fake a digital signature then for counter initiated transactions you are unable to disguise the fact you have tampered with the data even if you edit audit logs etc.

2.5 – as per previous comment.

3.3 – in 3.3.4 would change to testing controls more generally (one way of testing controls is walking through the processes)

3.4 – We did do some limited review of source code if you refer to the agreed procedures list.

4.1.1 – BRDB is ‘hosted on a’ central server, rather than is the central server

4.1.5 – should read ‘in the branch database’ rather than ‘Branch Data’.

4.2.1 – JSN is different to the digital signature. Digital Signature is a unique ‘hash’ applied to each message that can be checked to ensure accuracy and validity of the message. The JSN I believe signed by the digital signature and is used to support completeness. Plus if it is edited the digital signature will no longer match the message (I believe).

4.2.2 (b) – I think they are delivered via interface files from the remote locations which have header and footer records etc to check completeness. I don’t think they can be used to verify data integrity beyond completeness, which as we’ve highlighted previously means they are more vulnerable than counter generated transactions.

4.4.2 – ok, maybe reference that controls above in place in new Horizon?

5.1 – Doesn’t this contradict what you state elsewhere around global users and database superusers

6.1 – You are accurate with the number is 26 from what we have observed during our testing.

6.3.1&3 – Need to be careful to understand the difference between JSNs, digital signatures, and digital seals as explained in the report.

6.3.6 – We only have verbal representation they cannot amend activity logs. Also due to the MD5 message digest having being 'cracked' the digital seals are not necessarily reliable (but these are not the digital signature as per previous point).

6.5.1 – Not sure what you are getting at here? We have not looked at the interface routines at remote points in the dataflow to the counter infrastructure.

6.6.1 – As articulated earlier we haven't really affirmed either way whether they can amend activity / audit logs (FJ attest they can't however)

6.7 – This is probably true but as articulated earlier the SOD issue is more around access to the keys which would allow you to hide the fact you have edited the digital signature. I think what you may actually be referring to here is looking at whether any super users have been logged deleting transactions etc, such work likely requiring controls support to verify

Thanks,

Mark

**Mark Westbrook**

Senior Manager | Deloitte LLP

D: GRO M: GRO

GRO | [www.deloitte.co.uk](http://www.deloitte.co.uk)

---

**From:** Gribben, Jonathan [mailto:GRO]  
**Sent:** 03 November 2016 17:38  
**To:** Westbrook, Mark (UK - Manchester) <GRO>  
**Subject:** RE: Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report

Thanks Mark

**Jonathan Gribben**  
Managing Associate  
Bond Dickinson LLP

Bond Dickinson

Direct:  
Mobile:  
Office:

GRO

Follow Bond Dickinson:



[www.bond dickinson.com](http://www.bond dickinson.com)

---

**From:** Westbrook, Mark (UK - Manchester) [<mailto:GRO>]  
**Sent:** 03 November 2016 17:07  
**To:** Gribben, Jonathan; Parsons, Andrew; Keating, Lewis (UK - Leeds)  
**Subject:** RE: Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report

Sorry Jonny I've been in a pitch all day and have an engagement this evening. Lewis and I will turn this around ASAP tomorrow morning.

Thanks,

Mark

**Mark Westbrook**

Senior Manager | Deloitte LLP

D: [GRO](mailto:GRO) M: [GRO](mailto:GRO)

[GRO](mailto:GRO) | [www.deloitte.co.uk](http://www.deloitte.co.uk)

---

**From:** Gribben, Jonathan [<mailto:GRO>]  
**Sent:** 03 November 2016 10:45  
**To:** Westbrook, Mark (UK - Manchester) [[GRO](mailto:GRO)]; Parsons, Andrew  
<[GRO](mailto:GRO)>; Keating, Lewis (UK - Leeds) [[GRO](mailto:GRO)]  
**Subject:** RE: Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report

Mark, Lewis,

I attach the summary of your report that we are proposing to issue to Post Office. Please would you review it and let us know whether or not you disagree with any of the content. There are also a few questions for you highlighted yellow.

There is pressure to circulate the summary as soon as possible. Are you able to get back to me today?

Regards

Jonny

**Jonathan Gribben**  
Managing Associate  
Bond Dickinson LLP

*Bond Dickinson*

Direct:   
Mobile:   
Office:   
Follow Bond Dickinson:



[www.bonddickinson.com](http://www.bonddickinson.com)

---

**From:** Westbrook, Mark (UK - Manchester) [<mailto:GRO>]  
**Sent:** 02 November 2016 09:52  
**To:** Parsons, Andrew; Keating, Lewis (UK - Leeds)  
**Cc:** Gribben, Jonathan  
**Subject:** RE: Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report

Hi Andy,

On 1) It is fairly standard for audit logs to be editable. It is a common problem with audit logs as a concept that it becomes very hard to segregate them from the 'God' users, although on the most secure systems it can be achieved. Like the other data, the window of opportunity would be limited as Audit Logs are 'hoovered up' by the event management system and transferred to the audit store on a fairly timely basis (at which point they would become uneditable), just like everything else. As part of our work Fujitsu have implied the logs are segregated from the superusers, and so we could potentially look to test this if deemed of sufficient value?

On 2) I would imagine theoretically, but if limited to the branch database alone they would likely need to collude with other individuals such as other post masters as to actually extract money would in all likelihood require access to other systems. Finance system, Payments gateway etc.

On 3) We have identified the list of accounts which could (rather than has) breached SoD at the database level, but just trying to confirm with Fujitsu at the OS level as well. When we have the complete list and have vetted with Fujitsu, we will include within the report as an Appendix. In the interest of early clarity its more than 2 users.



Thanks,

Mark

**Mark Westbrook**

Senior Manager | Deloitte LLP

D: [GRO] M: [GRO]

[GRO] [www.deloitte.co.uk](http://www.deloitte.co.uk)

---

**From:** Parsons, Andrew [[mailto:\[GRO\]](mailto:[GRO])]  
**Sent:** 02 November 2016 08:29  
**To:** Keating, Lewis (UK - Leeds) <[GRO]>  
**Cc:** Westbrook, Mark (UK - Manchester) <[GRO]>; Gribben, Jonathan  
[GRO]  
**Subject:** RE: Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report

Lewis, Mark

A few (hopefully) quick questions.

In relation to Super-users, as I understand it, BRDB access is recorded in a separate audit log. The problem is that there are two super-users who can also access this audit log and could, theoretically, therefore change the BRDB and then change the log to cover their tracks. Perhaps a silly question by me but (i) why is the audit log editable at all and why is it not just read only and (ii) is there an audit of the audit log, that would should show someone has changed the audit log?

Do you know whether it would be possible for a super-user to change the BRDB in such a way that they could financially benefit? Eg. redirect payments to another account?

Do you have the names of the super-users at FJ who have broken the segregation of duties protocol?

Thanks

Andy

**Andrew Parsons**  
Partner  
Bond Dickinson LLP

*Bond Dickinson*

Direct: **GRO**  
Mobile:  
Office:  
Follow @bonddickinson



[www.bonddickinson.com](http://www.bonddickinson.com)

---

**From:** Keating, Lewis (UK - Leeds) [mailto:**GRO**]  
**Sent:** 31 October 2016 16:46  
**To:** Parsons, Andrew  
**Cc:** Westbrook, Mark (UK - Manchester)  
**Subject:** RE: Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report

Hello Andy

Please find attached a further draft of the Bramble report.

As always happy to discuss.

Thanks  
Lewis

---

**IMPORTANT NOTICE**

This communication is from Deloitte LLP, a limited liability partnership registered in England and Wales with registered number OC303675. Its registered office is 2, New Street Square, London EC4A 3BZ, United Kingdom. Deloitte LLP is the United Kingdom member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see [www.deloitte.co.uk/about](http://www.deloitte.co.uk/about) for a detailed description of the legal structure of DTTL and its member firms.

This communication contains information which is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please (1) notify [it.security.uk](mailto:it.security.uk@deloitte.co.uk) **GRO** by forwarding this email and delete all copies from your system and (2) note that disclosure,

WBD\_000342.000006

distribution, copying or use of this communication is strictly prohibited. Email communications cannot be guaranteed to be secure or free from error or viruses. All emails sent to or from a Deloitte UK email account are securely archived and stored by an external supplier within the European Union

To the extent permitted by law, Deloitte LLP does not accept any liability for use of or reliance on the contents of this email by any person save by the intended recipient(s) to the extent agreed in a Deloitte LLP engagement contract.

Opinions, conclusions and other information in this email which have not been delivered by way of the business of Deloitte LLP are neither given nor endorsed by it.

---

**From:** Westbrook, Mark (UK - Manchester)  
**Sent:** 20 October 2016 14:36  
**To:** Parsons, Andrew <[REDACTED]>  
**Cc:** Keating, Lewis (UK - Leeds) <[REDACTED]>  
**Subject:** RE: Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report

Hello Andy,

Please find attached a further draft of the Bramble report. We are still awaiting confirmation of segregation of duties around key management from FJ but that remains the only outstanding point.

Happy to discuss at your convenience,

Mark

**Mark Westbrook**

Senior Manager | Deloitte LLP

D: [REDACTED] M: [REDACTED]  
[REDACTED] | [www.deloitte.co.uk](http://www.deloitte.co.uk)

<< File: Bramble Draft 20102016.pdf >>

---

**From:** Westbrook, Mark (UK - Manchester)  
**Sent:** 10 October 2016 12:31  
**To:** 'Parsons, Andrew' <[REDACTED]>  
**Cc:** Keating, Lewis (UK - Leeds) <[REDACTED]>  
**Subject:** Private and Confidential - Subject to Legal Privilege - DRAFT Bramble Report

Hello Andy,

Please find attached the Draft Bramble report, updated version to be provided on conclusion of outstanding evidence areas from FJ.

Please do give me a call should you wish to discuss any aspects of the draft.

Thanks,

Mark

**Mark Westbrook**

Senior Manager | Risk Advisory | Deloitte LLP

P O Box 500, 2 Hardman Street, Manchester, M60 2AT, United Kingdom

D: GRO M: GRO

GRO [www.deloitte.co.uk](http://www.deloitte.co.uk)

<< File: Bramble Draft Report 10102016.pdf >>

**Please consider the environment! Do you need to print this email?**

---

The information in this e-mail and any attachments is confidential and may be legally privileged and protected by law. [markwestbrook](#) GRO only is authorised to access this e-mail and any attachments. If you are not [markwestbrook](#) GRO, please notify [andrew.parsons](#) GRO as soon as possible and delete any copies. Unauthorised use, dissemination, distribution, publication or copying of this communication or attachments is prohibited and may be unlawful.

Any files attached to this e-mail will have been checked by us with virus detection software before transmission. Bond Dickinson LLP accepts no liability for any loss or damage which may be caused by software viruses and you should carry out your own virus checks before opening any attachment.

Content of this email which does not relate to the official business of Bond Dickinson LLP, is neither given nor endorsed by it.

This email is sent by Bond Dickinson LLP which is a limited liability partnership registered in England and Wales under number OC317661. Our registered office is 4 More London Riverside, London, SE1 2AU, where a list of members' names is open to inspection. We use the term partner to refer to a member of the LLP, or an employee or consultant who is of equivalent standing. Our VAT registration number is GB123393627.

Bond Dickinson LLP is authorised and regulated by the Solicitors Regulation Authority.