POL00029103

Message

From: Mark Underwood1 GRO
Sent: 10/11/2016 12:16:21
To: Parsons, Andrew GRO
CC: Rodric Williams GRO
Subject: RE: Deloitte Report - Subject to Litigation Privilege

Thanks Andy – I think we need an agenda –even if we don't stick to it as Tom and Jane will expect something prior to the meeting

Sorry

Mark

From: Parsons, Andrew GRO
Sent: 10 November 2016 12:14
To: Mark Underwood1
Cc: Rodric Williams
Subject: RE: Deloitte Report - Subject to Litigation Privilege

I can do an agenda but Tony will simply say what he wants anyway! I'll speak to him on Friday and see if he has a plan.

Andrew Parsons
Partner
Bond Dickinson LLP

Bond Dickinson

Direct: GRO
Mobile
Office: GRO
Follow Bond Dickinson:

www.bonddickinson.com

From: Mark Underwood1 GRO
Sent: 10 November 2016 12:12
To: Parsons, Andrew
Cc: Rodric Williams
Subject: RE: Deloitte Report - Subject to Litigation Privilege

Really? Sounds a bit cloak and dagger?

Mark

From: Parsons, Andrew GRO
Sent: 10 November 2016 10:32
To: Mark Underwood1
Cc: Rodric Williams
Subject: RE: Deloitte Report - Subject to Litigation Privilege

POL00029103

No papers or agenda. We might circulate a draft letter if its ready.

A

Andrew Parsons
Partner
Bond Dickinson LLP
GRO

From: Mark Underwood1
Sent: 10/11/2016 10:04
To: Parsons, Andrew
Cc: Rodric Williams
Subject: RE: Deloitte Report - Subject to Litigation Privilege

Thanks Andy.

Separately – is there an Agenda or Papers for Monday's meeting with TRQC?

Mark

From: Jane MacLeod
Sent: 10 November 2016 09:34
To: Parsons, Andrew; Rodric Williams
Cc: Gribben, Jonathan; Mark Underwood1
Subject: RE: Deloitte Report - Subject to Litigation Privilege

That's helpful – I'm supportive of doing this further work as it goes to the heart of the issue.

Thanks Andy

Jane MacLeod
General Counsel
Ground Floor
20 Finsbury Street
LONDON
EC2Y 9AQ
GRO

From: Parsons, Andrew GRO
Sent: 10 November 2016 08:28
To: Rodric Williams GRO; Jane MacLeod GRO
Cc: Gribben, Jonathan GRO; Mark Underwood1 GRO
Subject: RE: Deloitte Report - Subject to Litigation Privilege

Jane, Rodric

We've spoken further with Deloitte. Although Deloitte are being cooperative, their risk management processes mean that answers are being vetted and this is taking us time to get forward progress. They have been able to clarify some further issues but the main point is that to get a clear picture they will need to undertake some more testing – see below.

POL00029103

Current position. The overall current position has not changed – there is a still a risk that super-users could change transaction data without leaving a footprint. However, the circumstances in which this could happen appear to be narrowing (because certain types of changes will be logged and those logs cannot be edited). The risk area appears to be around (i) spoofing digital seals and (ii) data in transit (ie. when it is travelling between servers).

Forward plan. Deloitte need to review the actual audit logs from Horizon. We originally put this work out of scope because it was not thought to be necessary given that we were not aware of the "segregation of duties" problem until the last minute. Reviewing the actual audit logs allows to points to be investigated:

1. Deloitte can look at what types of super-user activity are being logged and in what level of detail. This will hopefully allow them to answer the theoretical question about what types of super-user activity would not leave a footprint.

2. We can see whether any logged super-user activity has affected any claimant branches.

Next step. I'm asking Deloitte to cost up this option and I will then come back to you for approval.

Kind regards
Andy

Andrew Parsons
Partner
Bond Dickinson LLP

Bond Dickinson

GRO
Office: GRO
Follow Bond Dickinson:

www.bonddickinson.com

From: Parsons, Andrew
Sent: 07 November 2016 08:25
To: Rodric Williams; Jane MacLeod
Cc: Gribben, Jonathan
Subject: RE: Deloitte Report - Subject to Litigation Privilege

Jane, Rodric

Quick update.

We've put further questions to Deloitte but not yet had a full response. We are hoping to have the summary of the Deloitte report ready by tomorrow. It's currently with Deloitte for comments.

I'll let you know as soon as I know more.

Kind regards
Andy

Andrew Parsons
Partner

POL00029103

Bond Dickinson LLP
GRO

From: Parsons, Andrew
Sent: 02/11/2016 08:40
To: Rodric Williams; Jane MacLeod
Subject: Deloitte Report - Subject to Litigation Privilege

Rodric, Jane

As discussed yesterday, please find below the relevant extracts from the Deloitte report.

I've put the additional questions to Deloitte and will let you know as soon as I have answers.

Kind regards
Andy

Appendix 7:

Key questions

a) Whether Fujitsu can edit or delete transactions recorded by branches in a way that could impact on the branch's overall accounting position?

> *Yes – Transactions can be deleted at database layer (BRDB) by DBA's.*
>
> *Before audit store access locked down, transactions could be deleted at audit store level (and still can be once a transaction has been in the audit store for 7 years), but this would not affect a branches overall accounting position unless there was a query that resulted in the extraction of data. If data was extracted from the audit store and records had been tampered with or removed, this would be flagged upon extraction by the process to report on data integrity, so it would be transparent that the data has been edited. It should be noted the warning that the data integrity check failed can be ignored by the operator.*

b) How difficult it would be to do (a)?

> *Access to do (a) is restricted to appropriate personnel by Fujitsu. For users who have DBA access on the BRDB, this could be done.*
>
> *However if the edit/delete of the transaction was not done before the data had been 'collected' by the Audit Server (typically every 15 minutes), then this would not affect the record of data in the Audit Store. The audit store is the location where data is retrieved from in the event of a dispute.*
>
> *Further if the edit/delete of the transaction was performed prior to the data being 'collected' by the Audit Server, whilst it would be reflected in the audit store data, upon retrieval of branch data from the audit store, if a transaction had been removed, the 'data density' check would highlight a missing transaction. If upon retrieval of branch data from the audit store a transaction had been amended, the digital signature check would highlight an issue with the integrity of the data.*

c) Whether (a) is possible without leaving a "footprint" that is visible to either (i) postmaster or (ii) Post Office / FJ.

> *i) Amendment / deletion of transactions would not be overtly notified to the Postmaster, however if the amendment / deletion happened at the BRDB, this would affect the declarations made by Postmasters (encouraged to do so on a daily basis) and also declarations are required to be done in order to rollover into the next accounting period (typically 4-5 weeks). The monthly Branch Trading Statement which a Postmaster must sign off on in order to roll into the next accounting period would also be impacted by a change of this nature which would capture summarised totals of transactional data, which could be reconciled by branch back to the granular transaction log reports. All of the mentioned reports are mechanisms by which the Postmaster would be made aware of any such changes.*
> *Amendment / deletion of data in the audit store has no effect on branch accounting and would only impact a branch (Postmaster be made aware) if data was retrieved from the audit store. Further if upon retrieval of branch*

POL00029103

data from the audit store a transaction had been removed, the 'data density' check would highlight a missing transaction. If upon retrieval of branch data from the audit store a transaction had been amended, the digital signature check would highlight an issue with the integrity of the data.

ii) Branch Database privileged Oracle user operations are audited by Oracle to the SYS.AUD$ table. This table is extracted into audit files every night by a batch job into a directory from which the audit archiving system extracts the data. The audit data is currently stored for 10 years. This table can be extracted from the Audit Store by Fujitsu.

Any amendment / deletion of data in the audit store would be visible to Fujitsu only when data is retrieved. Upon retrieval of branch data from the audit store a transaction had been removed, the 'data density' check would highlight a missing transaction. If upon retrieval of branch data from the audit store a transaction had been amended, the digital signature check would highlight an issue with the integrity of the data.

As per the exception noted on page 3, there is a small theoretical risk of a user 'spoofing' the digital signature, arising from a failure in SOD controls relating to the digital signature.

d) Whether (a) has ever actually happened?

Audit logs of super-user access in the BRDB exist. Fujitsu have confirmed where amendment / deletion of live database tables would be identifiable from this log.

Our work has not included obtaining logs for the relevant time period and performing analytics over them to identify any instances where this has happened, and investigate if so. Such procedures should be theoretically possible however.

Page 3:

Access to mechanisms for managing the digital signatures are segregated from database administration responsibilities (via system access rights restrictions), meaning that even if such access rights be abused the digital signature that is included with every Counter and Kiosk transaction could not be spoofed. – *Relevant Exceptions Noted*.

The exception noted was

- *'A number of users have access to mechanisms for managing the digital signatures and have database administration responsibilities and access. This raises the theoretical risk of a user 'spoofing' the digital signature. It is understood that for this risk to be realised, due to time limitations and volume of work required in order to successfully 'spoof' the signature, a program would have to be written.'*

POL00029103

Andrew Parsons
Partner
Bond Dickinson LLP

Bond Dickinson

GRO
Office: GRO
Follow Bond Dickinson:

www.bonddickinson.com