WITN10500102

Confidential and subject to litigation privilege

ALAN BATES & OTHERS v POST OFFICE LIMITED

Privileged Users – Draft Executive Summary

1. The Claimants in the Group Litigation have asserted that Post Office / Fujitsu has the ability to add / delete / change transactions recorded by branches without the consent / knowledge of a postmaster and that this may have been the cause of discrepancies in some of the Claimants' branch accounts. We understand that the allegation has been formulated in several different ways:-

    1.1.1 Post Office / Fujitsu have the ability to log on remotely to a Horizon terminal in a branch so to conduct transactions.

    1.1.2 Post Office / Fujitsu have the ability to conduct transactions (either remotely or locally) under another user's ID.

    1.1.3 Post Office / Fujitsu have the ability to push transactions into a branch's accounts without either a postmaster's (a) knowledge or (b) consent.

    1.1.4 Post Office / Fujitsu have the ability to amend or delete transactions entered by branch staff on Horizon (and can do so in a way that is hidden from postmasters).

1.2 The way data was handled by Horizon materially changed in 2010 with the introduction of Horizon Online. Horizon and Horizon Online therefore need to be addressed separately.

Horizon Online

1.3 In simple terms, data input in branches is not stored locally on systems in branch. The data is sent on a transaction by transaction basis from the branch to the Branch Database (**BRDB**) which is a central Post Office server (hosted by Fujitsu). The BRDB then disseminates that data to various other places (such as Post Office finance systems, etc), including sending a copy to the Audit Store. The Audit Store is another server hosted by Fujitsu and is intended to be the master record of all branch transactions. In usual circumstances, it holds that data for 7 years.

1.4 When branch staff lookup transaction records, the terminal in branch contacts the BRDB to retrieve the necessary information. Given that branch accounts (as seen and operated in branch by postmasters) draw on data from the BRDB, additions, edits or deletions in the BRDB could impact upon branch accounts.

1.5 The integrity of transaction data (as recorded in branch and then communicated via the BRDB to the Audit Store) is protected in the following ways-

    1.5.1 Counter transactions (ie. those transactions that originate in branch due to the actions of branch staff) are given a unique number of 1 greater than the previous transaction so that the data can be checked for missing or duplicate transactions.

    1.5.2 Counter transactions are also digitally signed (i.e. a unique "hash" is applied to each message) so that the accuracy and validity of the transaction data can also be checked.

    1.5.3 Non-counter transactions (ie. those generated by Transaction Acknowledgements that originate from Post Office) must be confirmed by branch staff before they are accepted into the BRDB. Once accepted, a copy of the raw data file is also sent direct to the Audit Store.

    1.5.4 When data is sent from the Branch Database to the Audit Store via the Audit Server it is sealed (while in the Audit Server) and a database of sealed files is maintained so that when data is subsequently retrieved from the Audit Store, its integrity can be checked.

Commented [WM(-M1]: Database?

Commented [WM(-M2]: Not sure I'd agree with this?

Commented [WM(-M3]: 10 years now not 7

Commented [WM(-M4]: I think the raw data is just sent anyway?

Commented [WM(-M5]: Limitation of MD5 hashing algorithm?

WITN10500102

1.6 Setting aside the "remote access" issues discussed below, in our view:

1.6.1 the controls in Horizon are an effective way of ensuring that the transaction data input by branch staff (counter and non-counter) is recorded in the BRDB and Audit Store;

1.6.2 it is extremely unlikely (though not impossible) that the data input by branch staff and as recorded in the BRDB and the Audit Store would be incomplete or inaccurate;

1.6.3 in the event that data was incomplete or inaccurately recorded, the controls in Horizon provide effective tools for identifying such issues; and

1.6.4 therefore a suitably skilled and qualified person could review the raw data from the Audit Store to determine whether any data was incomplete or inaccurate.

1.7 In response to the allegations made at paragraph 1 above, we confidently believe that:

1.7.1 Neither Post Office nor Fujitsu have the ability to log on remotely to a Horizon terminal in a branch so to conduct transactions.

1.7.2 Neither Post Office nor Fujitsu have the ability to conduct transactions (either remotely or locally) under another user 's ID (unless that user shares their password but this would be a breach of operational procedure).

1.7.3 Neither Post Office nor Fujitsu have the ability to push transactions into a branch's accounts without either a postmaster's (a) knowledge or (b) consent, except for Balancing Transactions:

(a) BTs are visible in the transaction log produced in branch and are displayed using the unique identifier XXXX (which is different form the usual User ID that branch staff would expect to see).

(b) BTs do not require formal acceptance through the Horizon terminal by branch staff (unlike transaction corrections and transaction acknowledgements) and so can be pushed into the branch accounts by Fujitsu.

1.7.4 Fujitsu (but not Post Office) has the ability to amend or delete transactions entered by branch staff on Horizon – this is addressed below.

1.8 A limited number of authorised Fujitsu personnel have sufficient privileges to theoretically add / delete / change data in the BRDB (**Privileged Users**). These users may also have access to other systems, such as the Audit Store, however in the current circumstances access to the BRDB is the most important as it is the BRDB that generates the branch accounts and is the data used to hold postmasters liable for shortfalls.

1.9 Post Office personnel do not have this Privileged User access and we have seen no evidence to make us believe that they ever had such access, however there is no historic record of all the Privileged Users that there have ever been.

1.10 Changes to a branch's transaction data in the BRDB by Privileged Users would be visible to branch staff. The amended transaction would show up in a transaction log produced in branch but it would not be flagged as a change by a Privileged User and would appear like a normal transaction generated in branch.

1.11 We would expect a system such as Horizon to have this type of Privileged User access as it will be used to undertake maintenance on the system or to implement updates. Such access comes with a risk of it being misused, either by accident or maliciously. It is impossible to eliminate this risk entirely (within Horizon or any other IT system) and so systems generally have robust controls over the use of Privileged access so to reduce the risk or misuse or to make it detectable.

Commented [WM(-M6]: This was the proving a negative question. Given the procedures we have done I think we need to tone down wording somewhat.

Commented [WM(-M7]: This could be spoofed using the back end access we have been focusing on.

Commented [WM(-M8]: POs cannot do BTs directly?

WITN10500102

1.12 A key control in Horizon is the segregation of access permissions between Privileged Users who can access the BRDB and those users who may access the Key Management Server (**KMS**). The KMS holds the digital keys that underpin the controls listed in paragraph 1.5. Segregation of Privileged Users from KMS users ensures that a Privileged User cannot get around the controls in paragraph 1.5 and therefore cannot cover up any changes they make in the BRDB. If a proper segregation of duties is in place, any changes by a single Privileged User to the BRDB would be detectable in line with paragraph 1.6.4 above. This does not eliminate the risk of misuse entirely as there could be a conspiracy between a Privileged user and a KMS user.

1.13 Through our enquiries, we have identified that certain current Privileged Users **[how many?]** have access to the KMS such that they could theoretically cover up changes they make to the BRDB data. This is a failure by Fujitsu to implement its own segregation of duties policy. We are unable to determine how long this vulnerability has existed as records of historic users are not kept.

Commented [WM(-M9]: 32 we think but would need to check.

1.14 Despite this vulnerability, in our view it is extremely unlikely that actions by a Privileged User would be the cause of shortfalls in a branch.

1.15 First, Horizon has adequate functionality (in the form of transaction corrections and balancing transactions) to resolve the vast majority of imaginable operational errors in branch or technical errors in Horizon. There is therefore little need to use Privileged access to manipulate transaction data so to resolve an error – such use would be very rare and a last resort.

Commented [WM(-M10]: BTs themselves are an example of this functionality.

There is no perfect record of all Privileged User access, however our enquiries indicate that Privileged Users only access the BRDB approximately XX times per month. A sampling of the access logs shows that each access related to an authorised work order. None of those work orders required a Privileged User to change any branch transaction data (they related to wider system support). These enquiries therefore support the conclusion that Privileged User access is not being used to change branch transaction data as a matter of usual business practice.

Commented [WM(-M11]: TBD

[Moreover, since July 2015 Horizon logs the actions of Privileged Users If a Privileged User attempted to switch of the logging of their activities it would "break" the system. If a Privileged User tried to delete the log of their actions that would log a delete action (which would be highly unusual and therefore easy to spot), which means that a Privileged User could never completely covered their tracks.]

1.16 Second, any change to a branch's transactions in the BRDB by a Privileged User would be visible to Post Office, Fujitsu and branch staff and Fujitsu has the data and expertise to track down that the root cause of the change was the actions of a Privileged User. This means that should a Privileged User have incorrectly changed a branch's transaction data, it is very likely that it would be spotted and resolved.

1.17 Third, there is a theoretical risk of a Privileged User maliciously changing a branch's data and successfully covering up that fact that those changes were made by the Privileged User (due to Fujitsu's failure to segregate duties) but in our view this is a microscopically small risk:

1.17.1 The steps that would need to be taken for this to be successful are arduous and complex. Few people in the world would have the technical expertise to do this, it would require the writing of a bespoke computer programme, the circumvention of several other control measures and deployment of the fraud in a very small window of opportunity. We believe it would take weeks if not months of work and planning to pull this off successful.

Commented [WM(-M12]: Overly strong?

1.17.2 In light of the above, we cannot envisage any possible incentive or motivation for why a Privileged User would do this absent being involved in some form of massive criminal conspiracy.

WITN10500102

Old Horizon

[To be updated]