

---

**From:** Paula Vennells **GRO**  
**Sent:** Mon 29/10/2018 10:23:02 PM (UTC)  
**To:** Veronica Branton **GRO**  
**Subject:** Re: Board/ARC briefing

And you!!  
Thanks. P

Get [Outlook for iOS](#)

---

**From:** Veronica Branton  
**Sent:** Monday, October 29, 2018 10:20:57 PM  
**To:** Paula Vennells  
**Subject:** Re: Board/ARC briefing

Many thanks, Paula

That's gone.

Best wishes

Veronica

Get [Outlook for iOS](#)

---

**From:** Paula Vennells  
**Sent:** Monday, October 29, 2018 10:10:03 PM  
**To:** Veronica Branton  
**Subject:** Board/ARC briefing

Hi Veronica- please issue if poss. Sorry for the delay. Cc Ben Foat

Dear all,

**GRO**

We shall miss her around a few elements of the ARC/Board agendas, so I thought it might be helpful to explain beforehand - see notes below.

Any questions please ask me or Ben.

Best wishes,  
Paula

### **Board**

1) GLO: Common Issues Trial (CIT) commences next Monday. In Jane's absence, I have asked David Cavender QC (lead counsel) and Andy Parsons (lead lawyer from WBD) to come to the Board and brief us on the strike out judgement, 'tone of voice' challenge from the judge, claimants' draft CIT opening submission, and if we have time - Horizon trial preparation. We have made good progress on contingencies - Al can update.

2) LEO: we have simplified the proposal to a Post Office FS subsidiary and a Servco. Jane's ask is simple: the

Board agrees next steps of informing the FCA and that we work with Tom/colleagues to engage BEIS/SofS. The paper refers to approval for costs - not required as within limits.

3) UKGI Q3 report: apologies this was issued late - to allow for latest discussions with UKGI, a revised more granular format (and half-term holidays).

4) Banking Framework: oral update as this continues to be work-in-progress on rate card modelling, with a cut-off date in approx 10 days time.

## ARC

5) ARC Directors FYI: Jane would have provided some colour around the areas noted below. My thanks to Ben Foat (deputy GC) for the updates on live industry legal risks/read-across to Post Office and for a short summary on PCI status since the paper:

- PCI Non-Compliance: we have an technical solution (encrypting PCI-DSS at source (ie encrypting our PinPad estate)) which will take 9-12 months to deliver and cost approximately £8-£10m. We will seek to leverage/negotiate the front loading of this with Ingenico given that an upgrade would need to have been done in 4 years time. It is also important to note that there is no known security exposure because it is a closed system but POL will conduct a data audit by the end of the year to provide assurance regarding the security status whilst remediation measures are undertaken. Progress has been made remedying approximately 90% of the issues identified by the QSA. Legal has reviewed a sample of the key material contracts and confirmed that POL is in breach of its obligations to those upstream clients by failing to be PCI compliant and not notifying the material breach. A working group has set up to manage the issue going forward and particularly the notification to upstream clients (Banks, Utility companies, Bill Payment, Global Pay, etc) via our contract/business owners. Although breaching PCI does constitute a material breach, we consider that the upstream clients will obtain comfort through our technical solution, the remediation plan, and the fact that there is no security exposure and the broader commercial relationship. Consequently, we consider the risk of the upstream clients exercising termination to be low but we cannot rule out the risk.
- Morrisons: vicarious corporate responsibility for data breach – what necessary steps can POL take to prevent the unlawful processing of personal data arising from the unlawful actions of its employees. The backstop solution is that we have a cyber/ privacy insurance policy that covers this scenario. It would cover the compensation to claimants (settlement amounts) and defence costs up to £20m limit with a £250K excess. A cross functional working group (Compliance, HR, Legal etc) will be looking at the JML process and insider threat issue to consider what enhancements need to be made to our processes including SuccessFactors. This will include identifying super-users (SU), enhanced users and standard users and what restrictions should be in place; consider the Joining process when a role has been recognised or flagged as an SU role and make any modifications to that process if determined necessary; consider what continuous, if any, monitoring is applied to employees filling a SU role; ensure that when an employee moves internally to a SU role that any additional checks are made if required and ongoing monitoring is appropriate to the role; ensure that when an employee moves from a SU role that their access is removed and any additional monitoring is ceased ; and ensure that when an individual leaves the organization the Leavers process is fit for purpose.
- NDA Misuse: POL needs to ensure that it uses NDAs appropriately and they are not used to cloak, for example, criminal behaviour. The risk area that we will consider further is in relation to Whistleblowing. A member of the legal team is preparing a note on how we are using them and what enhancements (if any) may be needed. To give some comfort, the Solicitors Regulatory Authority (which is the regulator for Solicitors) has set guidelines for the use of NDAs which provides that NDAs are not prohibited and can be mutually beneficial to both parties. However, they should not be used to prevent disclosure to a regulator or law enforcement agency of a notifiable event including the SRA or as a means of improperly threatening litigation or other adverse consequences, or exerting inappropriate influence over people not to make disclosure which are protected by statute, or reportable to regulators or law enforcement agencies. This means that when the legal department is involved our regulatory duty to the law and our regulator cannot be trumped by the NDA but also we must ensure that they are utilised in an appropriate manner. The challenge will be to ensure that the business

understands when not to use the NDA e.g through the templates and training. Most often these are in relation to commercial arrangements which won't be an issue but it could arise a HR/ Whistleblowing context. We will provide a more detailed note with recommendations to our processes shortly.

· TIF: underwriter accused of neglect re vulnerable customers. POL's position is that there is no evidence (particularly in respect of post office customers) to support the allegations made by Mr Kingsbury. POI's internal investigation does not show any systemic issue with customer complaints or claims handling that would be out of alignment with the industry or our other provider Collinson. The Times have not indicated when they now proposed to publish. TIF have confirmed that they will be instituting legal proceedings against The Times in respect of their defamatory remarks to their suppliers. Comms and contingency plans are in place and we continue to monitor the situation.

Get [Outlook for iOS](#)