POL00423414

Compliance Report

Author: Jonathan Hill Sponsor: Jane Macleod Meeting date: 30 October 2018

Executive Summary

Context

This paper provides an update on the regulatory and compliance matters in respect of Post Office's financial services and telecoms businesses, financial crime and information protection and assurance.

We have included for the first time (in the Appendix) a consolidated compliance dashboard, which will continue to evolve and is intended to give the Committee with a snapshot overview of the compliance health of the business.

Questions this paper addresses

- What are the key compliance issues and what is the business doing to address these?
- What is the forward-looking regulatory agenda?
- What is the progress with the vulnerable customer action plan?
- What are the key policy updates in the period?

Conclusion

The key compliance risk areas are;

- Compliance with the Money Laundering Regulations and the remediation of Bureau de Change project requirements. We have already been fined by the HMRC for incorrect branch registrations and this area is being closely managed
- In Telco, breach identification and reporting is a concern, with fines (£1,000 per late report) being received for late reporting. The team has been to the HGS contact centre in Preston to investigate and are working with Fujitsu to implement changes to rectify the problem.
- Meeting the future regulatory agenda: there are a large number of items featured in the regulatory appendix and the regulatory discussion continues to evolve. Of particular focus this year have been the new General Condition requirements for Ofcom and the Insurance Distribution Directive which both come into effect in October and have required substantial work together with other parties and Principals to ensure compliance.
- Cyber Security and Cyber Crime: IT, Risk and Compliance have established a Cyber Defence Risk Assessment Forum to coordinate Post Offices approach to cyber issues.
- Vulnerable customers: We have set up a Vulnerable Customer Action Group (VCAG) to help track the work we are undertaking on vulnerable customers and to ensure that all parts of Post Office are joined up.
- Policy updates are included at the end of this report.

POL00423414

Input Sought

The Committee is requested to note this paper and approve the updates to the Vulnerable Customer and Anti Money Laundering & Counter Terrorist Financing policies.

POL00423414

Report

Contents

POL00423414

What are the key compliance issues and what is the business doing to address these?

Financial Services and Telecoms (including Banking Framework):

1. The key compliance issues are reviewed by Post Office Compliance and its partners at the BoI Customer & Conduct Risk Committee, POMS Joint Compliance Committee, the Banking Framework Security, Compliance and Governance Committee Compliance and the Telecoms Compliance Committee. The key items for each are reported below:

BoI/Post Office Customer and Conduct Risk Committee (CCRC)

2. The customer and conduct risks were reviewed at the September CCRC. The Committee reviewed the conduct risk metrics contained in the Post Office Distribution Conduct Risk Dashboards and agreed they were within appetite.

3. We continue to report one red metric (out of 12) for out of date literature, which includes provision of the Savings Summary Box leaflet to customers. We will continue focus on this whilst the products teams in BoI and Post Office develop more effective, paper-free solutions for providing customers with the necessary product information and application forms. This work is underway with a pilot savings application process being trialled on the CRM tablets. A Loans pilot is expected to follow shortly.

4. We have met with the BoI Vulnerable Customer Project Manager and have initiated quarterly meetings at a working level to communicate and where appropriate coordinate our efforts.

POMS/Post Office Joint Customer and Conduct Risk Committee (JCC)

5. The JCC meets monthly and reviews the conduct risk metrics contained in the Post Office Distribution Conduct Risk Dashboards to ensure they are within appetite.

6. As at 31st August, we continue to show two red metrics (out of 15). These relate CRM Easy Life Insurance mystery shopping results, which highlight a lack of conformance with the sales process. To address this, additional training has been and will continue to be provided to the CRMs and their supervisors. Changes were be made to the key health questions on the CRM tablets.

7. Calls to the Travel Insurance Contact Centre are being monitored to check for compliance to the new sales process which went live on 25th September with the implementation of IDD. Results for the first 3 weeks are showing 10,428 branch Travel Insurance sales, with 28 sales (0.27%) where the revised sales process was not followed. Horizon has been updated with the new process. Further MI including Branch codes has been requested to help support remedial activity.

8. Post Office travel insurance applications in branch have moved to an electronic version removing many of the risks we had with paper forms. Branches have been supplied with Customer Pads, which enable customers to write down their details if they do not want to give them to colleagues verbally. The information is given back to the customer at the end of the sale.

9. Mystery shopping results show colleagues across a number of branches are not actively talking to customers about products following a customer enquiry.

POL00423414

Network teams are working with branches to build product knowledge and confidence in conversations.

Banking Framework Security Compliance and Governance Committee (SCGC)

10. There were no material issues to raise with the banks and therefore it was agreed to cancel the meeting this month.

Telecoms Compliance Committee (TCC)

11. This new Committee held its second meeting at the beginning of September. The main focus of this meeting was on data breach reporting and identification. An action plan was agreed to address our concerns around identifying breaches, reporting breaches on time and supplying the necessary information.

12. The General Conditions changes were implemented in time for the 1st October start date. This has involved training the call centre on dealing with vulnerable customers, writing a new Customer Complaints Policy and updating the website to reflect the changes. Ofcom has confirmed it will not be checking that the changes have been implemented.

13. The focus will now move to the implementation of the S137 request from Ofcom, which requires significant system changes to be able to provide Ofcom with information next year for its quality of service report due in 2020.

14. The implementation of Expression of Dissatisfaction ("EoD") was deferred due to the General Conditions impact on the training pipeline. EoD is needed to improve our signposting score to the Alternative Dispute Resolution scheme. We are currently around 30-50%. Ofcom has set the industry an informal target of 90% by December 2018 (industry level is around 60%).

15. Work on the removal of Wholesale Line Rental ("WLR") to be replaced by fibre products and the regulatory implications is ongoing. This will form part of the telecoms' business strategy design over the next few months.

Customer Hub

16. The customer hub went fully live on 20th June with travel money and travel insurance. Since go live the monthly Enterprise Customer and Compliance Meeting ("ECC") has met regularly and reported in September that we have closed two risk exception notices relating to legal contractual risk exposure and the performance of the Travel App.

17. The ECC will seek to ensure that we obtain appropriate governance and control over tracking control issues whilst ensuring that we still remain part of an agile and digital working environment.

18. Going forward we are working with the hub team on compliant new propositions (e.g., mails) subject to business case approval.

Information Protection

Incidents

19. In the last month Post Office has seen a rise in the number of incidents that are being identified and reported, this is expected given the intensive training and awareness campaigns that we have run. The majority of these are within the Telecoms business because of the more stringent reporting requirements that exist for ISPs.

POL00423414

20. Additionally we have had four breaches from other areas of the business:

- Following on from a breach in Sodexo – our employee benefits portal provider – several members of staff have received targeted phishing mails. IT is working to block these and protect colleagues.
- An employee failed to follow the correct process and sent a daily banking transaction file to RBS meant for Lloyds Bank in an unencrypted state. An investigation is underway. No customer data has been lost as RBS acted quickly to inform us and understand the seriousness of protecting such data
- We reported a Post Office Insurance incident to the ICO & FCA, which involved the disclosure of limited personal data to another Post Office customer. The Data Protection team finalising its investigation. Actions are already being taken by POI and its contact centre provider (WebHelp).
- We identified a technical breach of our data controls, which occurred through an internal IT help desk operation run out of South Africa by Computacenter. The risk of actual data loss has been determined to be very low. We have also determined that there is no risk to people's rights and freedoms and thus have not notified the ICO.
    - We have notified some of our upstream contracts (e.g., Banking Services, Bill Payments and Government agreements) where they restrict personal data processing to within the EU/UK. We have had a number of follow correspondence and have had, to date, no negative responses.

Data Protection

21. Since the Committee met in July 2018 the number of Individual Rights requests has levelled out and we are now seeing similar numbers to those pre-May 2018. However, the requests that we are seeing are more complex and touching more parts of the business. We are monitoring this from a resourcing perspective.

PCI DSS

22. The Customer Hub Travel App has received its Attestation of Compliance from our QSA. This was required by FRES as there are direct links from the App into the FRES environment.

23. Please refer to the separate agenda item on PCI-DSS for details on the status for the rest of the estate.

ISO 27001

24. ISO 27001 is an industry standard that demonstrates an organisations maturity in managing information security.

25. The majority of our clients and partners expect us to be compliant to ISO 27001 and some of our contracts require certification for specific areas of the business and IT systems related to the services we provide on their behalf (for example UKVI and DVLA services through the AEI machines).

26. A successful Surveillance Visit 3 external audit was conducted between 24th and 26th July by Lloyds Register for the ISO27001 certification.

- We successfully closed the three findings that were raised during the last visit in January 2018.
- There was one Minor Non-Conformity raised, which both IT and Physical Security teams are addressing.

POL00423414

- The four branches selected by the auditor all demonstrated they were well organised and run, and only one incident observed where a branch assistant did not lock their Horizon terminal when away from the counter. This is a marked improvement from past audits.

Financial Crime

Compliance with Money Laundering Regulations

27. Annual AML/CTF training completion for back office staff as at mid-September was 98%.

28. As at 25th September, 59 branches remain outstanding. Details of these branches have been provided to Retail, and bureau de change services will be withdrawn from any branches that have not completed their training on 30th September. Two of these branches have been non-compliant since 2017 (their bureau de change service was switched off in October 2017) and these have been escalated to Contracts Managers as failure to complete their AML training also impacts contractual requirements for other products and services (e.g. MoneyGram and Banking Framework Services).

29. The new bureau de change data capability is identifying an increased volume of cases for review. Although monitoring reports have not yet been optimised or fully adopted, the number of issues identified is rising by c.40% per month, with 59 identified in Period 5.

    - A newly identified issue is agents/agent assistants processing transactions using their own personal details. Branches identified to date have been issued with a contractual remedy letter, and a branch communication was issued beginning of September.

30. As a result of the new data capability, we are seeing gradual increase in the identification of linked customer transactions over 90 days. There were 141 incidents identified from Period 4 to 25th September. This will be monitored over the coming months for regulatory and operational impacts as the new data capability beds in.

31. The volume of suspicious activity reports (SARs) in July, August and September 2018, was relatively stable (267, 242 and 200). With the new transaction monitoring and the ability to identify more unusual activity, reports relating to bureau de change are increasing and are at their highest levels ever (25-30% of all SARs).

    - We continue to identify suspicious high volume business banking deposits and liaise regularly with Santander as part of these investigations. As a result, Santander is looking to exit some client banking relationships.

Travel Money & HMRC

32. HMRC has formally responded to our letter relating to Customer Due Diligence and Fit & Proper, advising that it concurs with our interpretation of the CDD regulations. However we must provide changes to branch Fit & Proper data on a monthly basis. We continue to develop the data delivery and reporting capability to ensure we meet the regulations. There remain a large number of gaps in our agents' personal data. We are writing to all agents to remind them of the importance of providing this missing information and to receive agent's self-certification, which must be completed by 25th June 2019.

POL00423414

33. HMRC has started an audit of 50 branches (DMBs and agents) to check compliance with the Fit & Proper requirements. We have written to all branches in the post code areas that HMRC has selected. We will accompany HMRC on all visits. The first three visits were undertaken on 20th September. No significant issues were identified during these visits.

Anti-Bribery and Corruption (ABC) update

34. Annual ABC training completion is at 95% following the 21st August completion date. Non completion is being chased via HR.

35. The updated policy has now been approved by Post Office and POI ARCs and has been published on the Intranet. A One Communication is being arranged as a reminder of some of the key gifts and hospitality reporting messages.

Whistleblowing update

36. There are no material issues to report. The updated policy has now been approved by Post Office and POI ARCs and has been published on the Intranet. A One Communication is being drafted with the assistance of the People & Culture Director to remind all employees of the reporting channels available to them and to promote Post Office's open approach to supporting colleagues. A review of the Code of Business Standards has also been initiated.

Regulatory updates

37. Further to the launch announcement in 2017, the National Economic Crime Centre ("NECC") is being established this autumn and will take over responsibility for the National Crime Agency and the Joint Money Laundering Intelligence Taskforce ("JMLIT"). As part of the establishment of the NECC the Government has committed more resource for JMLIT, which will result in increased information requests and typology analysis for member institutions (of which Post Office is an active member).

External threats

38. We continue to see external attack in relation to iTune and Giftcard scams against vulnerable customers and branch communications have been issued as a reminder of the red flags to look out for.

Cyber Risk and Cyber Crime

39. As part of Post Office's on-going readiness approach to protecting our customers, clients and business, the IT, Risk and Compliance teams are working together to provide a coordinated approach to cyber risk and crime.

40. We have 12 security tools in place (please see appendix A) and receive a number of external fraud and cyber-related reports from partners etc.

41. We have now established a Cyber Risk Assessment Forum, reporting to the Information Security Committee, to coordinate these reports, on-going activities and propose future actions to keep the business safe.

    - As part of this work, we are reviewing the FCA's report on the recent Tesco Bank current accounts cyber-attack will be assessing our position against the FCA's findings.

POL00423414

What is the forward-looking regulatory agenda?

Please see the regulatory calendar in Appendix B.

Citizens Advice Super Complaint

42. On 29th September, Citizens Advice submitted a super-complaint about the 'loyalty penalty' to the CMA and FCA.

- Citizens Advice raised concerns about long term customers paying more for goods and services, which it refers to as 'the loyalty penalty'. It has identified five key markets where it has concerns about the loyalty penalty, covering telecoms and financial services. These are:
  - mobile
  - broadband
  - savings accounts
  - mortgages and
  - household insurance
- More details on the complaint and the related Ofcom and FCA activities are set out in Appendix C

43. Next Steps

- Post Office was invited to respond to the CMA's investigation as a telecoms provider. We submitted our response to the CMA, focusing on our telecoms business but offering to talk to the CMA about our other businesses if it would find this useful. The CMA has 90 days (late December) to respond to the super complaint.

Vulnerable Customer Action Plan

Listening and working with our stakeholders

44. We continue to engage with our stakeholders to ensure that we understand the challenges raised by their members and consider what improvements they would like to see. Most recently we met with the NFSP to understand and agree co-ordination on vulnerable customer initiatives, particularly 'dementia friends'.

45. We also recently met with Action on Hearing Loss (AHL) to understand their members' challenges and concerns. AHL reported that up to 80% of hearing loops tested across the industry were faulty. It was important to ensure that hearing loops once installed continue to be maintained to ensure tuning and functionality.

Key issues on the Work Plan

46. This includes what we have to do for regulatory or key stakeholder management (the must dos) this does not include work that we are already undertaking as part of our strategy such as POca or Identity.

- Branch Accessibility Guidance - Martin Hopcroft

  We had branch accessibility guidance in place (2014) but this needed updating. Following consultation with external accessibility consultants the 2014 guidance updates are being completed and a communication will be shared with the Network.

POL00423414

- Banking Framework 5 point plan-completed

  Point 4 of the five point plan (point 4) was to promote the Banking Framework including enhanced support for vulnerable customers following Citizen's Advice Guidance, which has now been completed.

- Ofcom - new vulnerable customer requirements October 2018: completed

  Ofcom required a number of vulnerable customer improvements to be put in place as part of the new General Condition requirements. We have implemented the changes as required and will be assessing the impact on a monthly basis.

- Alternative Format Literature - January 2019, Penny Smith FS&T

  For branch customers requesting alternative format literature for FS&T products (e.g., large print, braille, audio) the risk assessment identified that this process was broken.

  An action place is in place with FS&T requiring a third party supplier to provide alternative format literature and for call centres to be enabled with phone options to pass customers on to the third party provider. Call centre staff will also need to be trained on the new requirements.

- Telecoms Text Relay service - October 2018, Meredith Sharples

  A text relay service is used by customers on landlines with communication difficulties. We are currently making changes to these call charges.

- Training our staff – new Success Factors Vulnerable Customer Module - November 2018, Tracy Lloyd/Paul Beaumont

  We are currently reviewing the first draft of the new module. After undertaking user testing we expect to deliver this by the end of November.

- Communication on the Post Office Website - Phase 1 completed

  We updated and improved much of the content that was required on our social responsibility pages. This covers money advice for personal issues, money management/advice and advice on electronic safety and how to avoid scams. This includes signposting external sources of support.

Proposed Next Steps and the way forward

47. The next steps are to take forward the action plan across the Post Office and continue our work on vulnerability working with our stakeholders where required. As well as continuing to learn about best practice and keeping ahead of proposed regulatory changes.

Key Policy Updates

48. The Committee is asked to note the updates to the Vulnerable Customer and Anti-Money Laundering and Counter Terrorist Financing policies and give its approval to the revisions as part of the annual review process. The marked-up policies are attached in the appendices.

Vulnerable Customer Policy

49. The key changes to the policy are:

POL00423414

- New Policy Owners
- A definition of a vulnerable customer
- Update to some of the external references made in the policy
- Making it a requirement to consider consumer vulnerability when designing new customer propositions

The Anti-Money Laundering and Counter Terrorist Financing Policy

50. There are no material changes but amendments include:

- Error correction of prison term for tipping off offence (amended from two to five years)
- Reference to the new HMRC Fit & Proper Policy
- Clarification of minor points and updating external Whistleblowing contact details

Jonathan Hill

Compliance Director

22nd October 2018

POL00423414

APPENDIX A

Post Office Cyber Defences

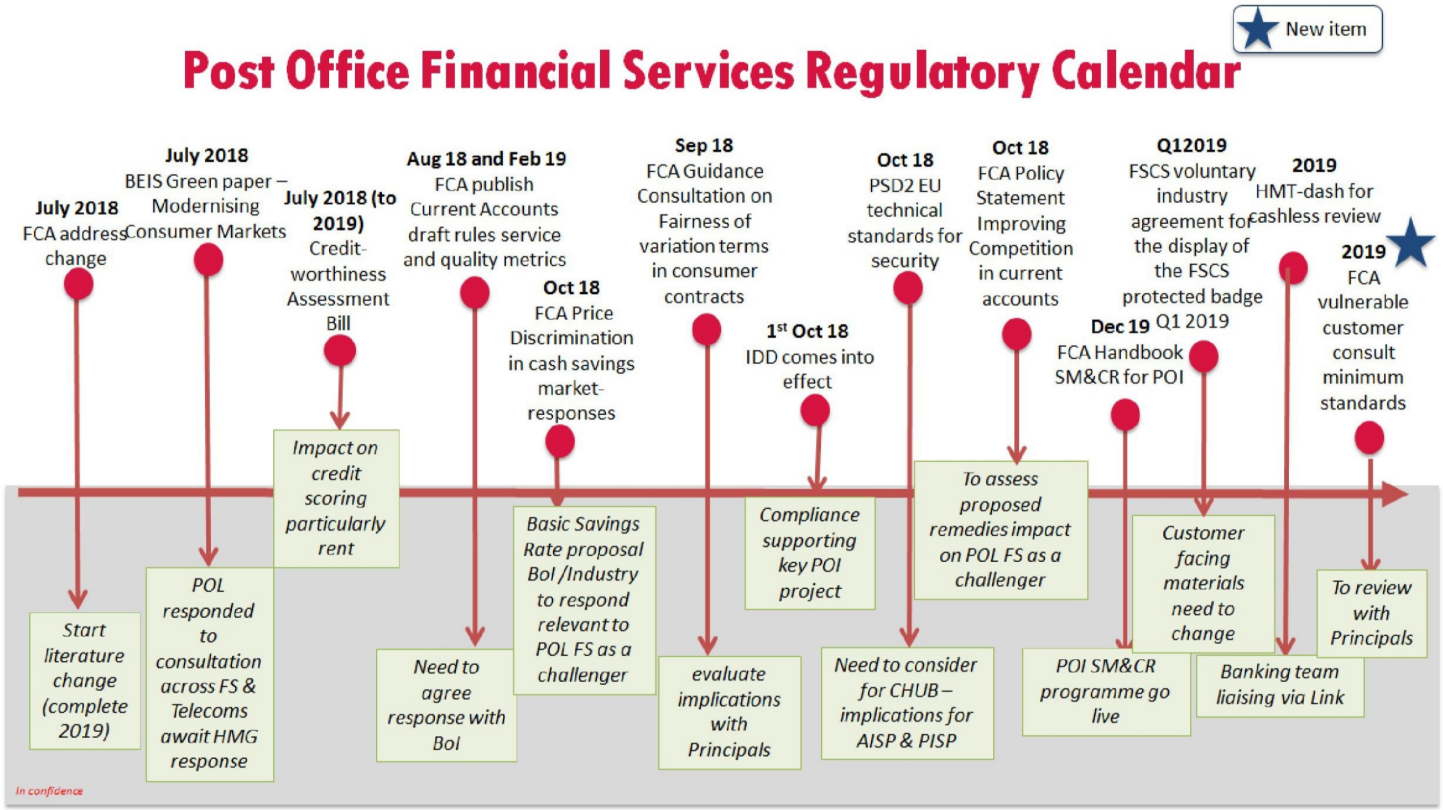
Active Security Deployments	How it protects us
Symantec	Endpoint security for laptops and datacentres (Antivirus)
Splunk	Detecting incidents and potential cyber breaches covering Verizon, Fujitsu, CC and Accenture
MS Intune	Protects corporate sensitive data on mobile devices
Ironscales	Protects employees from phishing attacks
Skybox	Protects our network perimeter from vulnerabilities and firewall misconfiguration
Digital Shadows	External dark-web scanning for Post Office information and artefacts
Mimecast	Email protection against malware
ZScaler	Protecting access to malicious or inappropriate websites that amplify malware attacks
Entrust	Certificate management to ensure we have increased visibility in security loopholes that can be exploited by hackers
AWS Shield	Protects against DDoS attacks via .co.uk interfaces
WAF	Protects our web applications (e.g., Travel Money) from malicious attacks
CISCO Meraki	Protects our Wi-fi estate from unauthorised access
24x7 Security Operations Centre	Brings all of the reports together and provides 24x7 active monitoring for cyber threats such as DDoS, Malware, Phishing, Ransomware etc.

POL00423414

APPENDIX B – REGULATORY CALENDAR

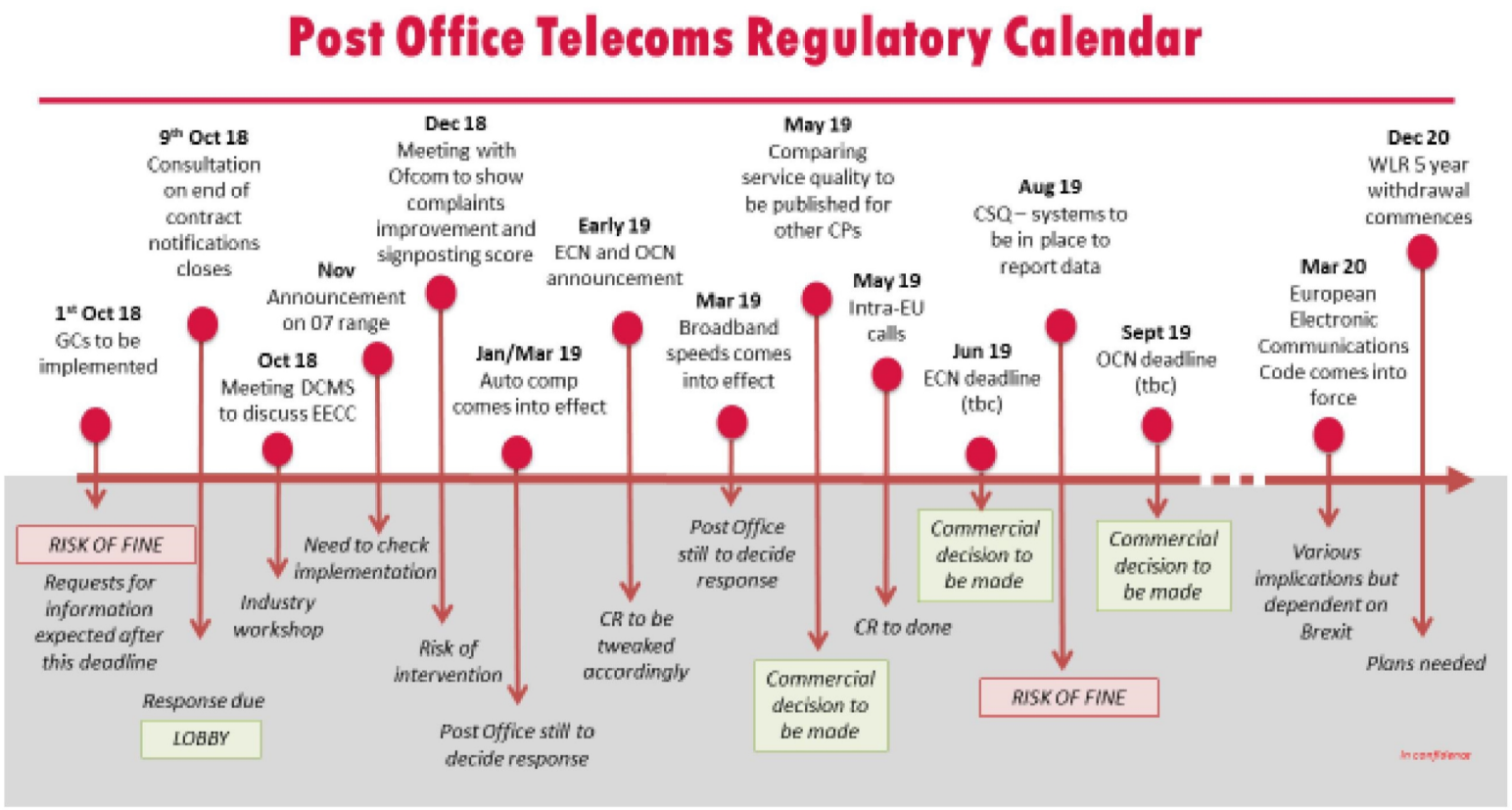
The diagrams below set out the key activities of the Financial Services and Telecoms regulators. As we develop this we will look to include calendars for Financial Crime and Information Security regulation.

Post Office Financial Services Regulatory Calendar



POL00423414

Post Office Telecoms Regulatory Calendar



POL00423414

APPENDIX C

Citizens Advice Loyalty Penalty Super Complaint

Citizens Advice Super Complaint

On 29th September, Citizens Advice submitted a super-complaint about the 'loyalty penalty' to the CMA and FCA.

- Citizens Advice raised concerns about long term customers paying more for goods and services, which it refers to as 'the loyalty penalty'. It has identified five key markets where it has concerns about the loyalty penalty, covering telecoms and financial services. These are:
  - mobile
  - broadband
  - savings accounts
  - mortgages and
  - household insurance
- The majority of the complaint outlines the research Citizens Advice has undertaken evidencing how long standing customers are discriminated against in favour of new customers. It acknowledges that regulators have made changes to the regulatory regime, but in Citizens Advice's view these have not been enough to mitigate consumer risk particularly those that have difficulty engaging in switching such as the vulnerable and older customers.
- It has asked the CMA to undertake a thorough, cross-sectoral market study into the penalty paid by loyal and disengaged consumers.
  - What more can be done to encourage consumers to engage in markets where the loyalty penalty exists?
  - What direct interventions into these markets are necessary to protect consumers from exploitation?
  - What specific protections for low-income and vulnerable consumers who pay the loyalty penalty are necessary?
- Citizens Advice argues that some form of price regulation is necessary, which appears to be an increasing trend in regulation (e.g., energy, telecoms, consumer credit, minimum savings rates)

Regulator activity – Ofcom:

- Given the focus by both government and Citizens Advice on the "loyalty penalty" (i.e. the difference between front book and back book pricing), Ofcom released a call for inputs document last year. It is concerned about the lack of "engagement" in the industry and that consumers are not shopping around for the best deal and has put forward various suggestions to rectify this.
- Following on from Ofcom's consultation and research it decided to focus on the introduction of end of contract notifications in broadband and also want all customers who are out of contract to receive a one off reminder that they could get a better deal. It is currently consulting on the format that this will take and we are engaged with Ofcom on this.

POL00423414

- This is an opportunity for Post Office, as it should create churn in the market although clearly there is a risk as we are effectively "waking up" the entire base. This is just the start and Ofcom have indicated to us that it may go down the route of caps, like Ofgem have done in energy, however it hopes it will not need to.

Regulator activity – FCA:

- Cash savings markets - FCA has issued a Discussion Paper outlining a proposal for a minimum savings rate for customers of over a year (Consolation Paper in 2019). This could have significant consequences for Post Office's savings pricing if implemented as proposed.
- Mortgages - The FCA is already undertaking work in this area and published an interim report in June 2018. It will publish more information later this year. This is aimed at facilitating switching, particularly customers that can be trapped in mortgages on SVR and are unable to re-mortgage, rather than price regulation.
- Insurance - A new rule was introduced under ICOBs two years ago requiring firms to disclose last year's premium at renewal (to facilitate shopping around) and to convey messages on switching.
- In the FCA's 2018/2019 Business Plan it announced that it would be looking at the pricing practices of general insurance firms. FCA have stated following today's announcement that it will launch a market study looking at how general insurance firms charge their customers for home and motor insurance. The terms of reference for this market study will be published in a few weeks' time.