BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Treasury Committee
House of Commons
London
SW1A 0AA

Lyndon Nelson
Deputy CEO
Prudential Regulation Authority

16 September 2019

Dear Chair

Treasury Select Committee Appearance: 24 July 2019
Oral evidence: IT failures in the financial services sector inquiry

I had promised during my TSC appearance at the above hearing, to provide the Committee with more details concerning examples of *"where the Senior Managers Regime or accountability structures have bitten firms that have not upheld their responsibilities"* particularly in the context of IT incidents/failures. This letter sets out the background to the Senior Managers and Certification Regime (SM&CR) and the relevant Senior Manager Function (SMF), which covers IT failures; and our enforcement process.

The SM&CR promotes good regulatory outcomes by strengthening the link between seniority and accountability. At its core, it requires the most senior decision takers (Senior Managers) to be assessed as fit and proper, have clearly defined responsibilities and be subject to enhanced conduct rules. We make significant use of the SM&CR throughout the supervisory "life-cycle" of approval, on-going supervision and enforcement. Given the nature of our work most of this activity remains confidential (under s348 of the Financial Services and Markets Act) with only approvals and enforcement typically becoming public.

The PRA introduced the Chief Operations Senior Management Function (SMF24) in November 2017. The SMF24 covers the most senior individual(s) responsible for "internal operations and technology of a firm". It was introduced to clarify and strengthen responsibility for a range of areas of increasing importance to the regulators' objectives including: business continuity; cybersecurity; information technology; internal operations or outsourcing. Given the recent introduction of SMF24 we do not have any public examples where the Senior Managers Regime or accountability structures have bitten firms in relation to IT failures; but this does not preclude us from doing so in the future.

Like other SMFs, the PRA and FCA assess the fitness and propriety of SMF24s and subject to the outcome of this assessment, approves them. The assessment of SMF24 candidates tends to consider their awareness of the financial regulatory landscape, including the regulators' increasing focus on operational resilience as well as their technical expertise of relevant areas, such as cyber or third-party risk management. Before being appointed to this position, individuals need to be

approved by the PRA and FCA. Since November 2017, 20 interviews for the SMF24 role have been conducted.

A number of firms have highlighted the positive impact that the introduction of the SMF24 has had on their governance. In particular, it compelled them to allocate clear responsibility at an appropriate senior level for areas such as cyber-security, which in the past may have been relegated to 'technical issues'. By doing so, firms improved board and executive committee engagement on these areas.

The Committee will be very aware of the substantial technological change that is happening in the financial sector and the very large investments that firms are making. As highlighted in Sam Woods' Mansion House speech last year, the PRA expects firms to designate one or more Senior Managers to be responsible for delivering on the supervisory priorities set out in its annual Periodic Summary Meeting letter. As part of this process, the PRA will discuss with firms how the success or failure to deliver against the objectives relating to the identified priorities may feed into remuneration awards. This includes ensuring that responsibility for major firm-specific deliverables is appropriately allocated to individuals, discussing the scope of their responsibilities and accountability throughout the supervisory lifecycle. These expectations are no different when addressing operational risks such as IT transformation that have been identified as posing risks to our statutory objectives and therefore supervisory priorities. Our supervisors have been active in seeking risk mitigation in terms of governance and project management where we see the risks to our objectives as being too great. The SM&CR has been a key tool for us in this effort – making sure that accountabilities are clear and are in the right place for investments and projects of this scale and that responsibilities are similarly clear.

Of course, being vigilant on approvals and active on-going supervision is not enough and we do make use of our enforcement powers. Outside of the SMF, the PRA has a strong track record of imposing sanctions where conduct by a firm and/or an individual (including the most senior individuals in a financial firm) could impair our ability to supervise them properly; or represents behaviour outside the bounds of what the PRA considers acceptable.

Current Investigations

Owing to the confidentiality provisions I mentioned before and related legislation, we are unable to provide specific details concerning current ongoing investigations. However, we can state that the current investigative portfolio include examples of the PRA looking for both firms and senior individuals to account for their actions in respect of matters that fall broadly under the banner of 'operational resilience'. This would include, but is not exclusive, to IT outages. These investigations focus on exploring potential weakness in oversight and control that may have contributed to the potential failures in addition to the role and responsibilities of senior individual(s) in the decision making and oversight of the potentially affected area.

It is important to be mindful of the fact that investigations are just that, an exercise to determine the factual chronology, events and causes of an incident. There may then be a determination as to whether, and if so which of, our rules have been breached. Our current investigative pipeline reflects our supervisory priorities. It also reflects the population of PRA firms under supervision: encompassing deposit takers and insurers; and the breadth of category of firms from one to five.

Finally, I wanted to thank the Committee for its interest in this area and also for the opportunity to write on this question of senior management accountability. As we know accountability is not the

same as culpability and the SM&CR is not a "strict liability" regime. However I wanted to re-iterate the point I made in oral evidence that we hold firms and individuals to account through a variety of regulatory and supervisory tools not all of which can be discussed in public. In many, arguably most, cases the PRA's various formal and informal supervisory tools, help promote and strengthen accountability when used as part of day-to-day supervisory discussions. The SM&CR has been a very important improvement in our ability to do that.

Yours sincerely

LWG Nelson

Lyndon Nelson
Deputy CEO, Prudential Regulation Authority