BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

FINAL NOTICE

To: **R. Raphael & Sons plc (FRN 161302)**

Date: **29 May 2019**

1. ACTION

1.1. For the reasons given in this Notice, the PRA imposes a financial penalty on R. Raphael & Sons plc ("Raphaels" or the "Firm") of £1,121,512 on the basis that the Firm contravened Fundamental Rules 2, 5 and 6 of the PRA's Rulebook during the Relevant Period.

1.2. The Firm agreed to settle at an early stage of the PRA's investigation, and therefore qualified for a 30% (Stage 1) discount pursuant to the PRA Settlement Policy. Were it not for this discount, the PRA would have imposed a financial penalty of £1,602,160.

2. SUMMARY OF THE GROUNDS FOR ACTION

Background

2.1. The Firm is an independent bank involved in the provision of banking and related financial services. The Firm is regulated by the FCA for conduct matters and the PRA for prudential purposes.

2.2. The Firm's business includes a Payment Services Division which issues prepaid cards and charge cards in the UK and Europe. As of 2016, the Firm had c. 5.3 million prepaid cards in issue in the UK and other European countries with average monthly transaction volumes of over £450 million.

2.3. The Firm contracts with outsourced service providers to provide services critical for the performance of its Payment Services Division. These outsourced critical services include: (i) the management of the Firm's card programmes by Card Programme Managers; and (ii) the authorisation of payment transaction requests from Card Payment Systems on behalf of the Firm (this service was itself sub-contracted by Card Programme Managers to Card Processors).

2.4. The Firm's risk appetite and tolerance levels are set by the Board. The Board is therefore ultimately responsible for setting the control environment throughout the Firm, including the appetite and tolerance levels in respect of outsourcing risk. The Board articulates the risks and tolerance levels the Firm is willing to accept through its Board Risk Appetite and Tolerance Statement ("BRATS"). This is intended to provide a common framework for the management of risk across the Firm. The Board bears responsibility for the effective management of all risks to which the Firm is exposed.

2.5. On 24 December 2015, the Firm brought the PRA's attention to an IT incident that had occurred earlier that day at a sub-contracted Card Processor (the "IT Incident"). The incident resulted in the complete failure of all services that Card Processor provided to the Firm for three Card Programmes. The IT Incident lasted over 8 hours, during which time 3,367 of the Firm's customers were unable to use their prepaid cards and charge cards. In total, 5,356 customer card transactions attempted at point of sale terminals, ATM machines and online (worth an aggregated value of £558,400) could not be authorised and were consequently declined. The IT Incident also prevented customers from viewing their contemporaneous card balances online.

2.6. Following the IT Incident, the PRA has investigated the Firm's arrangements for managing the risks associated with its use of outsourced service providers (including sub-outsourced service providers) in the provision of critical services.

2.7. More detailed information on the facts and matters relied on by the PRA in its decision-making process regarding the Firm can be found in Annex A.

Breaches and failures

2.8. The PRA considers that during the Relevant Period the Firm contravened PRA Fundamental Rules 2, 5 and 6 of the PRA's Rulebook[1]. This is because the Firm failed to appropriately and effectively:

(1) manage its outsourcing risk;

(2) instruct, oversee and monitor its outsourced service providers; and

(3) manage, oversee and monitor its business continuity and disaster recovery arrangements.

2.9. In particular, the Firm failed to manage its outsourcing risk appropriately and effectively because:

(1) The Firm had not established effective processes to identify, manage and monitor outsourcing risks and develop internal control mechanisms to address outsourcing risk.

(2) In particular, the Firm had not established an appropriate, consistent critical outsourcing risk appetite from Board level downwards. This was particularly important for the Firm to do given the heavy reliance it placed on outsourcing. The Firm also had no effective systems for monitoring how much outsourcing risk it was exposed to or whether the Board's risk appetite was being complied with. This prevented it from determining when its use of critical outsourcing exceeded the level of risk it was willing and able to accept.

2.10. The Firm failed to instruct, monitor and oversee its outsourced service providers appropriately and effectively because:

[1] Fundamental Rule 2 requires a firm to conduct its business with due skill, care and diligence. Fundamental Rule 5 requires a firm to have effective risk strategies and risk management systems. Fundamental Rule 6 requires that a firm organise and control its affairs responsibly and effectively.

(1) The Firm's initial due diligence and its ongoing monitoring arrangements for Card Programme Managers were inadequate particularly given the important role Card Programme Managers played in providing critical outsourced services and sub-contracting those services to Card Processors.

(2) The Firm's contractual agreements with Card Programme Managers failed to include appropriate service level agreements governing the provision of critical outsourced services.

(3) In relation to Card Processors, the Firm had no formalised initial due diligence requirements in place and its monitoring arrangements were flawed. The Firm was therefore almost entirely reliant on Card Programme Managers to identify and manage outsourcing risks related to Card Processors. The Firm failed to articulate its expectations of Card Programme Managers in carrying out this role or to ensure Card Programme Managers provided effective oversight of the functions outsourced to Card Processors.

2.11. The Firm failed to manage, oversee and monitor its business continuity and disaster recovery arrangements appropriately and effectively because:

(1) The Firm's business continuity and disaster recovery planning focussed only on services performed directly by the Firm notwithstanding the Firm's heavy reliance on outsourced services and the fact that the Firm bore ultimate responsibility for provision of those services.

(2) The cause and duration of the IT Incident reflected shortcomings in the Firm's understanding of the business continuity and disaster recovery arrangements of the impacted Card Processor. The Firm had no adequate processes for identifying and monitoring these arrangements, particularly how they would support the continued operation of the Card Programmes during a disruptive event.

(3) The Firm failed to investigate and respond appropriately when an earlier IT incident occurred in April 2014 at the same Card Processor which was later the subject of the IT Incident. If it had adequately investigated the April 2014 incident, the Firm may have been able to remedy the problems in the

Card Processor's business continuity and disaster recovery arrangements that increased the impact of the IT Incident.

2.12. As a result of the matters outlined at paragraphs 2.8 to 2.11 above, the PRA considers that the Firm:

(1) breached Fundamental Rule 5 because it failed (from Board level downwards) to have appropriate and effective risk management systems and strategies in place to deal with outsourced service providers. This failing was particularly acute given the Firm's significant usage of such providers;

(2) breached Fundamental Rule 6 because it failed to organise and control effectively its outsourcing of functions critical to the Card Programmes, in particular the Firm's business continuity and disaster recovery arrangements; and

(3) breached Fundamental Rule 2 because it failed to respond to the Initial IT Incident with sufficient due care, skill and diligence.

2.13. Further information regarding the Firm's breaches can be found in Annex B. Other requirements of the PRA Rulebook which underpin, and/or are supportive of, the breaches of Fundamental Rules 2, 5 and 6 are set out in full in Appendix 2 of this Notice.

2.14. For the reasons explained in this Notice, the PRA considers that there were failings in the Firm's systems and controls in respect of outsourcing which the Firm ought to have been on notice of from 18 April 2014. These failings crystallised on the date of the IT Incident and continued until the end of 2016, by which time the Firm had designed new outsourcing policies and outsourcing procedures to remedy the failings. Accordingly, the "Relevant Period" for the purposes of this Notice is 18 April 2014 to 31 December 2016.

2.15. The PRA acknowledges that during and since the end of the Relevant Period, the Firm, under a new senior management team, has taken significant steps to strengthen its outsourcing systems and controls. A report issued in December 2017 by a Skilled Person appointed by the Financial Conduct Authority concluded that Firm's design and execution of its outsourcing systems and controls broadly

enabled the Firm to comply with relevant outsourcing rules, subject to a number of recommendations.

3. REASONS WHY THE PRA HAS TAKEN ACTION

3.1. The PRA is responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers and major investment firms. The PRA's role is to promote the safety and soundness of those firms.

3.2. The PRA considers that how a firm outsources and oversees the outsourcing of critical services, including IT functions, is an integral part of the PRA's assessment of a firm's safety and soundness. It is central to operational risk and was particularly acute in this instance given the Firm's overall reliance on outsourcing in its business model.

3.3. Further, the PRA considers that how firms manage their response to operational disruption is critical to maintaining confidence in the business services they provide.

3.4. An authorised firm may outsource critical operational functions (for example, for reasons of efficiency or prudent financial management). However, it may properly do so only if it remains mindful of its regulatory obligations and gives due regard to the impact of the proposed outsourcing on its ability to meet, or continue to meet, such obligations. This duty extends to cover critical services provided by all critical outsourced service providers including sub-contracted service providers.

3.5. The PRA expects a prudently managed firm to carry out suitable due diligence on the counterparty to which it intends to outsource and to set appropriate parameters with regard to the division of responsibilities, as well as adequate arrangements for the oversight of the outsourced function, all of which should be properly documented.

3.6. The PRA also expects that effective Board and senior management oversight of a firm will include: identification and understanding of the firm's reliance on critical service providers; setting proper risk tolerances that are appropriately cascaded; and ensuring that its risk appetite is adhered to within the firm and by its critical service providers.

3.7. The PRA requires firms and groups to have a clear allocation of collective and individual responsibilities. Under the Senior Managers and Certification Regime (SM&CR), key decision-makers (known as Senior Management Functions (SMFs)) must be allocated responsibility for all the key areas and activities of a firm and remain accountable for them notwithstanding their ability to delegate aspects of these responsibilities where this is justified and appropriately overseen. This includes where firms outsource functions to other entities within the group and external third parties. Since November 2017, the PRA has required CRR firms to allocate responsibility for a firm's performance of its obligations under the Outsourcing Part of the PRA Rulebook to an SMF (see the Allocation of Responsibilities Part of the PRA Rulebook, rule 4.1(21)). The PRA expects the SMF with that responsibility to be accountable for the firm's overall policy and strategy in respect of outsourced operational functions and activities; as well as for compliance with the outsourcing requirements for these functions and activities, which are set out in the PRA Rulebook, EU Directives and Commission Delegated Regulations, and Guidelines and Recommendations issued by the European Banking Authority (EBA) and European Insurance and Occupational Pensions Authority (EIOPA).

3.8. The PRA has previously issued the Firm with a Final Notice dated 12 November 2015 for potentially putting its safety and soundness at risk by failing to manage its outsourcing arrangements properly. The PRA considers that a repeat failing by a firm where it has previously taken enforcement action is particularly serious even where the firm has taken some steps to remedy the situation.

3.9. Taking into account the facts and matters set out above and the relevant factors set out in the PRA's Penalty Policy, the PRA considers that the imposition of a financial penalty of £1,602,160 is a reasonable, appropriate and proportionate disciplinary measure in response to the Firm's breaches of PRA Fundamental Rules 2, 5 and 6. The Firm agreed to settle the matter at Stage 1 and therefore qualified for a 30% discount, resulting in a financial penalty of £1,121,512. The basis for this penalty is set out in Annex C.

4. PROCEDURAL MATTERS

4.1. The procedural matters set out in Annex D are important.

Miles Bake

Head of Legal, Enforcement and Litigation Division

for and on behalf of the PRA

ANNEX A – FACTS AND MATTERS RELIED UPON

Background

1.1. Raphaels & Sons Plc ("Raphaels" or "the Firm") is one of the UK's oldest independent retail banks. The Firm is engaged in the business of banking and related financial services. The Firm is authorised by the PRA and jointly regulated by the FCA and PRA. The Firm has a number of business divisions including Payment Services, Lending and Savings.

1.2. The Firm is a principal member of the Visa and MasterCard Card Payment Systems and, through such membership, has become increasingly engaged in the market for the provision of prepaid cards and charge cards.

1.3. Prepaid cards can be used to make certain electronic payment transactions. Unlike credit and debit cards, they are not linked to an underlying credit facility or current account. Instead, a firm receives funds in advance before issuing e-money of an equivalent value onto the card. Common examples of prepaid cards include travel money cards, gift cards and payroll cards.

1.4. Similarly, charge cards can also be used for the making of electronic payment transactions. A credit limit is granted by the Programme Manager which can then be drawn upon by the card user.

Card Programmes

1.5. The Firm provides companies and other organisations seeking to launch new prepaid card or charge card programmes ("Card Programmes") with access to Card Payment Systems such as Visa or MasterCard.

1.6. The Firm's responsibilities in relation to Card Programmes include registering the programme with a Card Payment System, obtaining a Bank Identification Number from the relevant Card Payment System to enable payments to be authorised, and continually managing the settlement of payment transactions to the Card Payment System. At all times, the Firm also retains ultimate regulatory responsibility for managing the Card Programmes appropriately and effectively.

1.7. The Firm's Payment Services Division (the "PSD") manages operational responsibilities in relation to the Card Programmes. The PSD relies heavily on outsourced service providers to perform many of the services and functions which are critical to the operation of the Card Programmes. These outsourced service providers primarily include Card Programme Managers and Card Processors.

1.8. The Firm contracts with Card Programme Managers directly. A Card Programme Manager's contractual obligations are set out within a formal contract (a "Card Agreement"). These obligations include procuring a Card Processor, customer relationship management, product marketing and ensuring that sufficient funds are held in the accounts supporting the Card Programme for daily settlement with the card payment systems. In addition, the Firm and the Card Programme Manager agree a "Joint Operating Manual" setting out key operational procedures.

1.9. The Firm does not contract with Card Processors directly to set out all their obligations in respect of a Card Programme. Instead, a contract is agreed between the relevant Card Programme Manager and the Card Processor. The services provided by a Card Processor are predominantly IT services which include daily transaction reporting, fraud management monitoring and Payment Authorisation Services. The services to be provided by a Card Processor are detailed in both the Card Agreement and the Card Processor's agreement with the Card Programme Manager. The Card Programme Manager selects a Card Processor with the Firm confirming that appointment.

1.10. The Firm does enter into a "Compliance Agreement" with each Card Processor. This is primarily intended to ensure that the Firm can take control of a Card Programme if, for example, the relevant Card Programme Manager became unresponsive. In particular, Compliance Agreements enable the Firm to instruct a Card Processor directly to decline a specific transaction or set of transactions.

Critical Outsourcing - Appetite and Identification

Firm Risk Appetite

1.11. The Firm's approach to managing risk is governed by its Risk Management Policies and Procedures. A fundamental purpose of the Risk Management Policies and Procedures is to assist staff members with identifying and assessing risks. The

Risk Management Policies and Procedures identify the Board as the ultimate decision-making body with responsibility for determining the Firm's overall risk appetite and tolerance levels.

1.12. The Board articulates the risks and tolerance levels the Firm is willing to accept through its Board Risk Appetite and Tolerance Statement ("BRATS"). This is intended to provide a common framework for managing risk across the Firm. The Board bears responsibility for the effective management of all risks to which the Firm is exposed.

1.13. Both the Board and Executive Committee play important roles in the overarching governance and risk management of the Firm's outsourcing arrangements. These include: approving outsourcing relationships the Firm proposes to enter into; assessing management information regarding the Firm's ongoing monitoring of outsourced service providers; and reviewing key policies governing the Firm's use of outsourcing.

1.14. At the time of the IT Incident, the Risk Management Policies and Procedures explicitly identified "Outsourcing" as one of four principal risks for which the Firm needed to hold capital. Outsourcing risk was not specifically identified in BRATS. The PRA understands that the Firm's approach was to articulate outsourcing risk as a category of operational risk.

1.15. However, the description of operational risk within BRATS did not explicitly refer to the risks of outsourcing (including critical outsourcing) nor to the use of outsourced service providers. Instead, the PRA understands that outsourcing risk and the tolerance levels accepted by the Firm for specific outsourcing risks were impliedly captured by general references in BRATS to preventing "operational losses" and "compliance failures". BRATS referred to only one specific outsourcing risk: namely, the concentration risk of one Card Programme Manager contributing more than 25% of the Payment Services Division's gross profit (i.e. a risk to profitability rather than business continuity).

1.16. BRATS also referenced "IT Risk", noting that a business continuity and disaster recovery plan had to be in place and up to date with hardware and software maintained at levels consistent with those required for the Firm to meet its objectives. However, this reference related to the Firm's internal IT systems and

had no relation to the business continuity and disaster recovery plans of its outsourced service providers.

Business Division Risk Appetite

1.17. In addition to BRATS, the Firm's business divisions produce separate Divisional Risk Appetite and Tolerance Statements ("DRATS"). DRATS are intended to provide more detail about risks to each business division and their corresponding tolerance levels. The Risk Management Policies and Procedures provided for DRATS to be reviewed at least every six months by the Executive Committee and annually by the Board.

1.18. The PSD had a DRATS throughout the relevant period (the "PSD DRATS"). The PSD DRATS included some specific risks associated with outsourcing. However, like the BRATS, the PSD DRATS did not address the PSD's overall appetite for outsourcing critical services. Likewise, reference within the PSD DRATS to business continuity as a risk concerned the PSD's testing and remediation of its own business continuity plan and not the arrangements at outsourced service providers.

Outsourcing Policy

1.19. The Firm has had a documented "General Outsourcing Policy" (the "Outsourcing Policy") in place since January 2012. The version in force at the time of the IT Incident was dated December 2014. The Outsourcing Policy described itself as a "master framework" intended to guide the drafting of all outsourcing agreements. Both the Board and Executive Committee approved the policy.

1.20. The Outsourcing Policy listed the general outsourcing requirements under SYSC 8 of the FCA Handbook, stating a need to "understand fully the implications involved" and "ensure and control any outsource agreement in the manner prescribed by the Regulator". The Outsourcing Policy required all staff to take regard of and apply the SYSC 8 rules in their dealings with third parties.

1.21. The Outsourcing Policy emphasised the need for the Firm to monitor the performance of outsource service providers through "comprehensive Service Level Agreements". Failure or lapse in an outsourced service would need to be

corrected within an "agreed and reasonable timescale" given the "urgency and importance of the service as dictated in the Service Level Agreement".

1.22. However, other than reciting the general outsourcing requirements, the policy provided no additional guidance for the Firm's staff on how to apply the requirements in practice. In particular, the Outsourcing Policy provided no guidance on how to identify critical outsourced services, including how they could be distinguished from non-critical services.

1.23. The Outsourcing Policy referenced specific intra-group outsourced functions and services (i.e. functions and services outsourced to other entities within the same corporate group as the Firm) which required service level agreements (such as HR recruitment and commercial marketing services). However, the Outsourcing Policy did not provide equivalent guidance on which *external* outsourced functions or services required service level agreements.

1.24. None of the Firm's Card Agreements with its Card Programme Managers included comprehensive service level agreements expressly required under the Outsourcing Policy. In particular, the Card Agreements did not include service levels for the critical outsourced services required to operate a Card Programme.

1.25. The separate contracts agreed between the Card Programme Manager and the Card Processor did contain some service level agreements relating to the provision of critical outsourced services. However, the Firm had no involvement in setting or approving these. As a result, certain service levels agreed between the Card Programme Managers and the Card Processor did not align with the Firm's requirements.

Critical Outsourcing – Business Continuity and Disaster Recovery

The Card Agreements

1.26. All Card Agreements in force at the time of the IT Incident required the Firm and the relevant Card Programme Manager each to maintain a written business continuity plan to be made available to the other "upon request from time to time". Each business continuity plan was required, at all times, to include a "time frame for recovering critical business functions".

1.27. Under the Card Agreements, each party was also required to ensure that its "key suppliers" maintained their own business continuity plans. Again the suitability or parameters of the business continuity plans was not stipulated. The business continuity plans maintained by Card Processors were to be made available to the Firm for inspection upon request.

1.28. The Card Agreements did not require the business continuity and recovery arrangements of Card Programme Managers and Card Processors to align with or meet the Firm's requirements.

1.29. Each Card Agreement set out the essential services that the Card Programme Manager was to procure that the Card Processor would provide "on a timely basis". These included, among others, Payment Authorisation Services and the "provision of production & disaster recovery data centres". Specifically, they required:

(1) the production environment to be "fully resilient" and with "no single point of failure";

(2) a "disaster recovery site" to be in place which was annually tested and which replicated the production data centre;

(3) a "business continuity plan" to be in place; and

(4) that services could be recovered within "4 hours".

1.30. However, these specific requirements covered only those services provided by the Card Processor. Other than the need to maintain a business continuity plan, there were no similar requirements in the Card Agreements for Card Programme Managers and the services they directly performed.

The Firm's continuity and recovery arrangements for critical outsourced services

The Firm's Business Continuity Plan

1.31. At the time of the IT incident, the Firm had in place a central business continuity plan (the "Firm BCP"). The Firm BCP was reviewed by the Board and Executive Committee. Its principal purpose was to provide clear instructions to staff to enable continuity of service to the Firm's customers and suppliers. It described the types of disruptive incident which required its invocation, the procedures to be followed by staff and the locations of alternative disaster recovery sites.

1.32. The BCP required risk assessments for each of the Firm's "business lines and major operating functions" and that each of its operating divisions maintain separate business continuity plans. Each operating division was required to undertake a business impact analysis ("BIA") at least annually. BIAs were intended to identify and document the key risks to business continuity within a division. As part of formulating BIAs, each division was required to specify appropriate recovery time objectives and maximum tolerable downtimes for its "critical functions". A Recovery Time Objective was the timeframe for restoring services to a level where the Firm's reputation or its financial condition was not significantly impacted. Maximum Tolerable Downtime was the time after which the Firm's viability could be irrevocably threatened if product and service delivery could not be resumed.

1.33. The Firm BCP required each of the Firm's operating divisions to identify "its key business partners" and to "document appropriate contact details in its own BCP". In the case of "Outsourcing Partners", each contract was required to include specific sections on business continuity and disaster recovery. The contract required written confirmation from the outsourced service provider that an "up-to-date, fully documented and tested" business continuity plan was in place. Crucially though the Firm BCP did not stipulate that the business continuity plans of outsourced service providers had to adhere to certain minimum levels. Nor did it provide for Firm to approve the adequacy of those plans or ensure they were linked to the PSD's recovery time objective or maximum tolerable downtime figures.

The Third Party Business Continuity Management Questionnaire

1.34. The Firm BCP appended a "Third Party Business Continuity Management Questionnaire" (the "BCP Questionnaire") designed to assess the adequacy of the business continuity plans of "key" outsource service providers. The BCP Questionnaire sought details including the timeframe for recovery of services provided to the Firm and the mitigation strategies in place to prevent disruption to services.

1.35. However, the Firm BCP stated that not all suppliers and outsourced providers would be willing to complete the BCP Questionnaire. In those circumstances, how a division (e.g. the Payment Services Division) obtained the information was stated by the Firm BCP to be at the discretion of management.

1.36. The BCP Questionnaire did not seek any details of the relevant arrangements of or stipulate minimum criteria required of sub-contractors (e.g. Card Processors) providing critical services to the Firm. This was particularly significant given the questionnaire was not intended to be completed by sub-contractors. In addition, certain questions sought only "examples" of procedures for managing service disruptions rather than all procedures covering the key services provided for the Firm.

1.37. The Firm had not implemented any guidance for those reviewing responses to the BCP Questionnaire and the supporting evidence provided. This was particularly significant, given that staff responsible for reviewing the responses had not received business continuity training. Moreover, despite the heavy reliance on outsourced providers' technology for the supply of many key services, the Firm had no process for undertaking an informed assessment of the technological aspects of the questionnaire."

1.38. The BCP Questionnaire contained important questions concerning business continuity and recovery for outsourced services. However, the BCP Questionnaire was not completed by all directly contracting outsourced service providers (e.g. Card Programme Managers) notwithstanding the criticality of the services they performed on behalf of the Firm. The BCP Questionnaire was not completed by any of the Card Programme Managers impacted by the IT Incident.

The Payment Services Division's Business Continuity Plan

1.39. The Payment Services Division maintained a separate PSD business continuity plan (the "PSD BCP"). This detailed the specific actions the PSD would take to minimise the impact of a major disruption to its normal day-to-day operations. As required by the Firm BCP, the PSD BCP included a BIA (including relevant recovery time objective and maximum tolerable downtime levels) of its key systems and functions. However, this only considered internal systems and functions, and did not include consideration of any outsourced functions.

1.40. The PSD BCP expressly noted that it did not seek to address all of the possible business continuity planning scenarios that the PSD or its suppliers may experience. The PSD BCP stated that this was "covered in part" by the PSD requiring all Card Programme Managers to have their BCP open for inspection and less than one year old; by the Joint Operating Manuals detailing operating procedures; and by using major blue-chip technology providers for its major programmes.

1.41. Neither the Firm BCP nor the PSD BCP contained any actions or procedures relating to the continuity and recovery of outsourced services and functions during a disruptive incident. Only services performed directly by the Firm were considered in the plans, notwithstanding the dependency placed on outsourced services and the impact that disruption to those services could have on the Firm and its customers.

1.42. The PSD BCP did not address any possible business continuity scenarios that its outsourced service providers might experience. The PSD BCP contained no procedures for what, when and by whom communications with outsourced service providers would take place in the event of an incident.

1.43. Although the Joint Operating Manuals described the services, including critical outsourced services, required for the operation of a Card Programme, they provided no details of how the continuity of such services would be maintained in the event of disruption. In particular, the Joint Operating Manuals gave no details of the recovery timeframes, available workarounds, minimum acceptable service levels or communication procedures required to manage disruption to outsourced services. Accordingly, the PSD BCP was wrong to describe the Joint Operating

Manuals as covering – whether in part or in any way at all – any of the possible business continuity planning scenarios that the PSD or its suppliers might experience.

1.44. The absence of any outsourced services or functions from the business continuity plans also meant that such services and functions were not included within the PSD's BIA. Therefore, the Firm undertook no assessment of the impact which disruption to these services or functions might have on it or its customers. Furthermore, it undertook no criticality assessment of the relative importance of these services and functions (including the assignment of appropriate recovery time objectives and maximum tolerable downtimes) to the business of the PSD.

The Firm's due diligence of outsourced Card Programme arrangements

Initial due diligence

1.45. From March 2012, the Firm's process for appointing a Card Programme Manager required the prospective Card Programme Manager to submit an initial due diligence form to the PSD's Business Development team. Amongst other things, the form requested a copy of an up to date business continuity plan and details of when it was last tested. The Business Development team and the PSD's first line compliance team shared responsibility for reviewing the form.

1.46. Each of the Card Programme Managers impacted by the IT Incident underwent an initial due diligence exercise prior to the launch of their Card Programmes. As part of this, the PSD undertook a review (albeit it is not clear against what criteria) of two of the three Card Programme Managers' business continuity plans submitted with their initial due diligence forms. However, both reviews were high-level, providing little indication of which continuity and recovery arrangements were assessed, if at all, or how they satisfied the Firm and the PSD's requirements.

1.47. For the third Card Programme Manager, the PSD did not undertake an initial review of business continuity or recovery arrangements. Had such a review been undertaken, the Firm would have identified that the Card Programme Managers' business continuity plans contained no "time frame for recovering critical business functions" as required by the relevant Card Agreement.

1.48. The PSD undertook a separate initial due diligence exercise before entering into a relationship with a Card Processor. There was no written policy or guidance as to what information should be initially requested from a potential Card Processor. In practice, the Firm sought to obtain similar information to that requested from prospective Card Programme Managers. The absence of a written policy meant that there was no formal requirement to initially assess a Card Processor's business continuity and disaster recovery arrangements.

1.49. In 2014, prior to the launch of one of the Card Programmes, the PSD undertook an informal review of the business continuity plan of the Card Processor impacted by the IT incident after the Card Processor had been appointed. The reviewer identified several "issues", including that the plan was over a year old and that the Card Processor's BIA was not made available. Significantly, the reviewer also noted that the plan could not be invoked for "day to day system failure" and that this gave "some cause for concern". The PRA has seen no evidence indicating that this concern was followed up prior to the IT Incident.

On-going monitoring

(i) Annual due diligence form

1.50. Once a Card Programme had been launched, the PSD would conduct ongoing due diligence of the Card Programme Manager by having it submit an annual due diligence form. The form did not seek details of the current business continuity and recovery arrangements of a Card Programme Manager or those parties it had sub-contracted services to.

1.51. The annual form was not sent to, nor did it mention, Card Processors. Instead, the Firm relied on its Card Programme Managers to conduct ongoing due diligence of Card Processors. The Firm did not stipulate in any of its contractual arrangements with Card Programme Managers any parameters as to how this due diligence should be undertaken.

(ii) Outsource Monitoring Reviews

1.52. The PSD also conducted Outsource Monitoring Reviews ("monitoring reviews") of each Card Programme Manager. Monitoring reviews were carried out in

accordance with the Firm's Outsource Monitoring Procedures. Monitoring reviews were designed, among other things, to ascertain the extent to which each Card Programme Manager adhered to its policies and procedures and complied with regulatory requirements. Whilst the Outsource Monitoring Procedures did not specify any particular regulatory requirements, certain monitoring reports included some consideration of compliance with SYSC 8.

1.53. The Firm had initially intended for a monitoring review of each Card Programme Manager to be completed annually. In practice, however, the Firm sought to concentrate on the Card Programme Managers considered to pose the greatest risk to the PSD and the Firm. This risk based approach adopted by the PSD meant that not all Card Programme Managers received an annual review. Crucially, the initial risk assessment which informed this approach did not consider whether any of the services provided by the Card Programme Manager constituted critical outsourcing for the purposes of applicable regulatory rules.

1.54. In addition, resourcing constraints within the PSD prevented certain Card Programme Managers from receiving a review as scheduled. Consequently, PSD could not ensure that all Card Programme Managers providing critical outsourced services received a timely monitoring review.

1.55. The PSD's Outsource Monitoring Procedures expressly mentioned business continuity management as a potential review area. In addition, the agenda template used to formulate the specific agenda for each monitoring review included reference to "BCP" and "BCP Results". However, beyond these references, the procedures gave no guidance or criteria on how to assess business continuity plans and their test results. This was because the PSD had no such guidance in place.

1.56. The absence of any guidance or criteria meant that business continuity plans were not reviewed against clear requirements set by the Firm, including the recovery objectives set out in the PSD's BIA. This created a risk that recovery timeframes set by critical outsource service providers, were not aligned with the PSD's objectives. In some instances, no review of business continuity, resilience or disaster recovery planning had taken place during the monitoring review, despite the Card Programme Managers being responsible for the provision of critical outsourced services.

1.57. In the year preceding the IT Incident, two of the three impacted Card Programme Managers received a monitoring review (the other Card Programme Manager had last been reviewed in June 2014). Each review included a desk-based review of policy and procedure documents.

1.58. The monitoring review report for each visit identified that the Card Programme Managers were not adequately monitoring the activities of the Card Processor and in one instance it was identified that the Card Processor had not been verified as required by the PRA Rulebook. However, neither review considered or reported on the Card Programme Managers' business continuity and recovery arrangements. Furthermore, no business continuity plans or disaster recovery plans were included in the desk-based document reviews.

1.59. Accordingly, the Firm undertook no review of the Card Programme Managers' respective business continuity plans in the year prior to the IT Incident. As a result, the Firm was not aware that two of the Card Programme Managers' plans had not been updated since 2012 and 2013 respectively, thereby contravening the PSD's requirement that outsourced service providers' "BCPs should be less than 1 year old".

1.60. In addition, Card Programme Managers were contractually required to ensure that the Card Processor maintained a business continuity plan (albeit not what form this should take or minimum criteria this should contain). The Firm also relied on Card Programme Managers to ensure that testing of the Card Processor's disaster recovery plan had been carried out. However, the Outsource Monitoring Procedures made no provision for how to assess whether the Card Programme Manager had satisfied these requirements.

(iii) Operational reviews

1.61. Prior to the IT Incident, the PSD had begun conducting annual "operational reviews" of its Card Programme Managers. These reviews looked at various operational activities integral to a Card Programme, such as card transaction reconciliation and account management.

1.62. In 2014, the PSD's procedure for conducting operational reviews highlighted the need to identify all business continuity plans supporting a Card Programme and

how the Card Programme Manager reviewed the plans of their sub-contractors (e.g. Card Processors). However, the procedures gave no guidance on whether, how and against what criteria this information needed to be evaluated.

1.63. Between 9 June and 25 July 2015, the Firm's compliance function carried out a review of the PSD's management of its outsourcing arrangements. The review culminated in a report issued by Compliance in September 2015. Compliance found that the PSD was not tracking Card Programme Managers' testing of their business continuity plans to ensure they remained fit for purpose. Compliance also found that the PSD were not testing how Card Programme Managers maintained oversight of sub-contractor business continuity plans. Its report noted that the PSD would incorporate these requirements into its operational reviews.

1.64. Prior to October 2015, the PSD tested its new approach to operational reviews on the main Card Programme Manager impacted by the IT Incident. However, the approach appears to have provided for only a limited inquiry into the Card Programme Manager's business continuity planning arrangements and prompted no changes to those arrangements. At the time of the IT Incident, the Card Programme Manager's business continuity plan was over two years old and contained no time frame for recovering critical business functions.

Initial IT Incident

1.65. On 18 April 2014, a "major incident" occurred with a Card Processor's systems supporting the Payment Authorisation Services provided to the Firm (the "Initial IT Incident").

1.66. Significantly, the Card Processor's description of the Initial IT Incident explained that:

(1) a weakness existed within the Card Processor's 'high availability' setup preventing its IT system from continuing to operate in the event of disruption;

(2) the duration of the incident was extended due to the Card Processor having to manually restart its IT system;

(3) the "normal" incident management and communication processes had not been executed properly by the Card Processor; and

(4) the incident impacted 57 customers across two of the Firm's Card Programmes (these two Card Programmes were also impacted by the IT Incident).

1.67. The Card Processor reported that the Initial IT Incident was an "unexpected eventuality" and that it had been addressed. However, the Firm appears to have taken no steps to investigate its underlying cause nor to review the adequacy of the Card Processor's business continuity and disaster recovery arrangements to manage similar future incidents.

1.68. Following the Initial IT Incident, the Firm and Card Processor agreed to hold a monthly meeting to discuss service provision, negative experience and reporting measures.

1.69. In the month following the Initial IT Incident, the Firm met with the Card Processor. At that meeting, the Card Processor explained that a "client alert system" had been created to notify clients (including the Firm) of future incidents. The Card Processor explained that its staff were "actively monitoring" for such incidents and that notification would be made by email or SMS. No further remedial steps were taken.

The IT Incident

Overview

1.70. During the early hours of 24 December 2015, an incident occurred at the same Card Processor resulting in the "complete failure" of the services it provided to the Firm for three Card Programmes (the "IT Incident"). The services impacted by the IT Incident included the Card Processor's provision of Payment Authorisation Services.

1.71. The IT Incident lasted for over eight hours and resulted in 3,367 of the Firm's customers being unable to use their prepaid cards and charge cards. Over the course of that period, 5,356 customer card transactions attempted at point of sale

terminals, ATM machines and online, worth an aggregated value of £558,400, could not be authorised by the Card Processor and were consequently declined. The IT Incident also prevented customers from viewing their contemporaneous card balances using the Card Processor's online portal. In addition, certain services utilised by the Firm and its Card Programme Managers to manage cards were disabled until the IT Incident was resolved.

Cause of the IT Incident

1.72. The root cause of the IT Incident was a malfunctioning of two of seven Database Instances at the Card Processor's production data centre. The two Database Instances impacted managed the customer and transaction data required for the provision of Payment Authorisation Services.

1.73. The Database Instances were intended to provide high availability, thereby ensuring the continuous provision of Payment Authorisation Services. However, the nature of the IT Incident was such that the high availability of the two Database Instances was compromised, resulting in all services associated with them (including Payment Authorisation Services) being brought to a halt.

1.74. The Card Processor's disaster recovery system, which would have enabled Payment Authorisation Services to be resumed from a secondary data centre, could not be initiated. This was because the Card Processor's disaster recovery plan had assumed that all seven Database Instances had to be down (i.e. a complete data centre failure) before the disaster recovery system could be initiated. This left the Card Processor with no other option but to manually create a system in order to restore Payment Authorisation Services. This task took over seven hours to complete, which breached the Firm's four hour recovery time objective for the recovery of Payment Authorisation Services.

1.75. The Firm was not aware that the provision of Payment Authorisation Services to its customers was supported by only two of the Card Processor's seven Database Instances. Therefore, the Firm did not know that Payment Authorisation Services could be disrupted (and the Card Processor's disaster recovery system could not be initiated) when only those two Database Instances had malfunctioned.

1.76. As a result of the Initial IT Incident in 2014, the Firm was or should have been aware that even a partial disruption to Database Instances at the Card Processor's

production data centre could impact the supply of Payment Authorisation Services. The Firm was also on notice that the Card Processor's business continuity plan would not be invoked for day-to-day system failure.

1.77. However, neither the Firm nor the Card Processor had conducted a business continuity or disaster recovery test in circumstances where only some Database Instances malfunctioned. As a result, no formal workarounds or contingency plans were in place to deal with a disruption of this nature.

1.78. Moreover, the Card Processor had no effective procedures for communicating with the Firm or the Card Programme Managers in the event of a disruption to its services. The incident started at 04:22 AM (GMT) but the Firm was not made aware of the disruption nor its consequent impacts until 09:00 AM (GMT). Had the Firm been alerted earlier, it could have taken steps to mitigate the impact of the IT Incident sooner.

1.79. Following the Initial IT Incident in 2014, the Card Processor had implemented an alert system to notify clients of disruption via email or SMS. However, the alert system was also disabled by the malfunctioning of the two Database Instances.

1.80. Following internal discussions, the Card Processor decided to notify the impacted Card Programme Managers. The notification was made by the Card Processor's Operations team at 07:15 AM (GMT). The Firm was not included in the notification and was subsequently informed by two of the Card Programme Managers at 09:00 AM (GMT).

1.81. Of the three Card Programmes affected by the IT Incident, the greatest impact was borne by a prepaid Card Programme issued predominantly to seasonal workers to provide their weekly wages. On the day of the incident, communications from a total of 1,121 customers were received, the vast majority of which related to the incident. These communications included complaints from customers who were unable to withdraw money, pay their bills or use their prepaid cards for Christmas shopping.

1.82. The Card Programme Manager offered these customers the option to receive up to £250 in an alternative bank account. To facilitate this, the Card Programme Manager requested that funds were released from its own account with the Firm.

The Card Programme Manager also placed an alert on its website and sent text messages to customers to update them on the disruption. These were impromptu measures initiated by the Card Programme Manager and approved by the Firm. They were not part of any formal business continuity plan.

Actions taken by Raphaels following the IT Incident

1.83. Immediately following the IT Incident, the Firm requested the Card Processor produce a full incident report identifying the root cause of the incident, the corrective action required to minimise the likelihood of it happening in future and the key lessons learned. Remedial action taken by the Card Processor included procuring additional hardware to bolster the high availability of its Database Instances and implementing a new communications plan to better manage future incidents.

1.84. In early 2016, the Firm self-commissioned an external firm to assess its outsourcing governance arrangements and, separately, its resilience and disaster recovery arrangements, against the applicable regulatory requirements in the FCA's Handbook and the PRA Rulebook. The assessments placed particular focus on the PSD's outsourcing.

1.85. The external firm's findings and corresponding recommendations were set out in two reports, both dated 30 June 2016. The reports identified a number of areas where the PSD's management of outsourcing risk was deficient, recommending significant enhancements to achieve regulatory compliance. In particular, the reports identified gaps and weaknesses in the PSD's "contingency and business continuity planning" in relation to outsourced services.

1.86. In response to the reports, the Firm implemented an outsourcing remediation plan. The purpose of the remediation plan was to design and implement a new governance and controls model to address the shortcomings in the Firm's outsourcing arrangements. The design phase of this plan was completed at the end of 2016, with implementation beginning in January 2017. Through the remediation plan, a number of significant changes have been made to the Firm's outsourcing framework, foremost among them:

(1) identifying outsourcing risk as a standalone risk in the Firm's BRATS;

(2) the introduction of new end-to-end outsourcing procedures for managing the risks to its critical outsourced services;

(3) revised due diligence procedures for Card Programme Managers to ensure a more comprehensive and holistic assessment is undertaken;

(4) enhancements to the assessment and management of the business continuity plans for critical outsourced service providers; and

(5) the allocation of first-line responsibility for the Firm's outsourcing to a Senior Management Function (SMF) holder.

1.87. In April 2017, the FCA required the Firm to appoint a Skilled Person to assess whether the Firm was compliant with the FCA's outsourcing rules. The Skilled Person's assessment considered outsourcing activity across the Firm and was carried out in two phases. The Skilled Person collated its findings from both phases in a final report issued in December 2017. The report concluded that the Firm's design and execution of its outsourcing systems and controls broadly enabled the Firm to comply with applicable regulations.

ANNEX B – BREACHES AND FAILINGS

1. FAILINGS

1.1. As a result of the facts and matters set out in Annex A, the PRA considers that during the Relevant Period the Firm breached Fundamental Rules 2, 5 and 6 of the PRA's Rulebook.[2]

1.2. The Firm's failings can be broadly categorised as follows. The Firm failed to:

(1) manage outsourcing risk appropriately and effectively;

(2) instruct, oversee and monitor outsourced service providers appropriately and effectively; and

(3) manage, oversee and monitor business continuity and disaster recovery arrangements appropriately and effectively.

1.3. For a brief part of the Relevant Period (from 18 April 2014 until 19 June 2014), the relevant high-level rules of the PRA Rulebook in force were the Principles for Businesses. However, for the purposes of this Notice, the PRA has focused on the Fundamental Rules as they were the applicable standards for the large majority of the Relevant Period.

Management of risks associated with outsourcing

1.4. During the Relevant Period, the Firm breached Fundamental Rule 5 because, from Board and Executive Committee downwards, it failed to set clear risk appetites in relation to the outsourcing of critical services and ensure that these risk tolerances were appropriately cascaded and adhered to both within the Firm and in the arrangements between the Firm, Card Programme Managers and Card Processors. It also failed to set out how to identify when it was relying on outsourced service providers for the performance of critical functions. In particular:

---

[2] Fundamental Rule 2: A firm must conduct its business with due skill, care and diligence.
Fundamental Rule 5: A firm must have effective risk strategies and risk management systems.
Fundamental Rule 6: A firm must organise and control its affairs responsibly and effectively.

(1) While operational risk was identified as a risk to the Firm's activities, the Firm failed to adequately articulate outsourcing risk within its Firm-wide (i.e. the BRATS) and divisional (i.e. the DRATS) risk appetite statements. The absence of a clearly defined outsourcing risk appetite meant the Firm could not determine when its use of critical outsourcing exceeded the level of risk it was prepared to tolerate. This was particularly relevant given the Firm had outsourced numerous services and functions which were critical to its activities.

(2) Both the BRATS and the DRATS had set risk appetite and tolerance levels for IT risk and business continuity which were confined to internal systems and did not include outsourced service providers. Consequently, when assessing a critical outsourced service provider's IT and business continuity arrangements, neither the Firm nor the PSD could determine whether those arrangements satisfied or exceeded an accepted level of risk.

1.5. As a result, the Firm lacked an effective system for monitoring or managing the critical outsourcing risk it was exposed to or, crucially, whether the Board's risk appetite was being complied with.

Instruction, oversight and monitoring of outsourced service providers

1.6. During the Relevant Period, the Firm breached Fundamental Rule 5 because it failed to organise and control its outsourcing activities effectively and failed to instruct, monitor and conduct appropriate oversight of its outsourced service providers. In particular:

(1) The Firm failed to exercise due skill, care and diligence when entering into, arrangements for outsourcing the performance of critical operational functions. The Firm's processes for initial due diligence of Card Programme Managers and Card Processors involved inadequate consideration of their business continuity and disaster recovery arrangements, and there was no policy on what information about these should be obtained from Card Processors.

(2) The Firm's Outsourcing Policy offered no guidance to staff on how to identify critical outsourced services, including how they were to be distinguished from non-critical services. As a result, the contractual arrangements with Card

Programme Managers failed to include appropriate service level agreements, and those service level agreements that were in place between Card Programme Managers and Card Processors were not aligned with The Firm's own requirements. This meant the Firm was unable to establish adequate service level agreements commensurate of the Firm's needs and/or adequate methods for assessing the standard of performance of these outsourced service providers.

(3) The Firm's risk-based assessment of how frequently monitoring reviews should take place took no account of the criticality of the outsourced services. Resourcing constraints meant that the Firm failed even to conduct the reviews its flawed assessment process had identified it should.

(4) In relation to Card Processors, the Firm failed to ensure that it had effective control of critical outsourced services. The Firm did not subject Card Processors to formal operational reviews, monitoring reviews or require them to complete annual due diligence forms (as stipulated in the Firm's guidance). Initial due diligence requirements for Card Processors were not formalised. The Firm was therefore almost entirely reliant on Card Programme Managers to identify and manage outsourcing risks related to Card Processors. However, the Firm failed to adequately articulate its expectations of Card Programme Managers in performing this role (or what its expectations were for Card Processors), for example by specifying what annual due diligence should be carried out. The Firm therefore failed to ensure that Card Programme Managers properly supervised the carrying out of the functions outsourced to Card Processors and adequately managed the risks associated with the outsourcing.

Business continuity and disaster recovery arrangements

1.7. During the Relevant Period, the Firm breached Fundamental Rules 2 and 5 because it failed to take reasonable steps to ensure the effectiveness of its own disaster recovery and business continuity arrangements and those of its critical outsourced service providers.

1.8. The Firm's business continuity and recovery planning (including its BIAs) was inadequate in that it was solely focussed on the services and functions performed directly by the Firm and not by providers of critical outsourced functions. Given

the criticality of the outsourced services to the continuous performance by the Firm of the relevant services and activities, it was essential for the Firm to ensure that corresponding arrangements were in place at its critical outsourced service providers.

1.9. The Firm BCP and the PSD BCP did not address business continuity in relation to outsourced services. This meant that there was no BIA in relation to outsourced, or critical outsourced, services. In addition, there was no adequate process for obtaining information about business continuity and disaster recovery arrangements at Card Programme Managers and Card Processors. Moreover, PSD staff responsible for assessing such information on an ongoing basis received no specific training or guidance on how to assess such information.

1.10. Further, the Firm failed to take proper steps in response to the Initial IT Incident to investigate its underlying cause and the impact on its customers. The Firm also appears to have taken no steps to review the adequacy of the Card Processor's business continuity and disaster recovery arrangements to manage similar future incidents. Had the Firm responded to the Initial IT Incident with due care, skill and diligence, it may have identified, and remedied, the problems with the Card Processor's business continuity and disaster recovery arrangements that contributed to the impact of the IT Incident.

ANNEX C – PENALTY ANALYSIS

1. FINANCIAL PENALTY

1.1. The PRA's policy for imposing a financial penalty is set out in '*The PRA's approach to enforcement: statutory statements of policy and procedure March 2019*, in particular *Statement of the PRA's policy on the imposition and amount of financial penalties under the Act* (the "PRA's Penalty Policy"). Pursuant to the PRA's Penalty Policy, the PRA applies a five-step framework to determine the appropriate level of financial penalty.

1.2. In addition, the PRA has also had mind to the level of the financial penalty that the Financial Conduct Authority has decided to impose in this case.

Step 1: Disgorgement

1.3. The Firm derived no economic benefit, profit made or loss avoided from the breaches. The Step 1 figure is therefore £0.

Step 2: The seriousness of the breach

1.4. In order to determine the starting point figure for a financial penalty the PRA may as set out in the PRA's Penalty Policy (paragraph 18) have regard to the seriousness of the offence and a suitable indicator of the size and financial position of the firm.

1.5. Having established an appropriate starting point figure the PRA then applies an appropriate percentage rate ("the Seriousness Percentage") to the starting point figure that properly reflects the nature, extent, scale and gravity of the breaches.

1.6. The PRA considers that the Firm's revenue for FY 2016 (being the financial year preceding the date when the breaches ended) is a suitable indicator of the size and financial position of the Firm. Accordingly, the starting point figure is £11,444,000.

1.7. The PRA has taken the following factors into account to determine the Step 2 Seriousness Percentage:

(1) The PRA considers that how a firm outsources critical services, including IT functions, is an integral part of the PRA's assessment of a firm's safety and soundness. It is central to operational risk and was particularly acute in this instance given the Firm's overall reliance on outsourcing in its business model.

(2) The breaches reflected serious and systemic weaknesses in Raphael's governance and controls relating to critical outsourced services.

(3) While the duration of the IT Incident was relatively short, lasting approximately eight hours, the breaches underlying the IT Incident had existed for a longer period of time over the Relevant Period before the risk they created ultimately crystallised and caused customer detriment.

(4) The PRA also expects effective Board and senior management oversight of a firm to include identification and understanding of the firm's reliance on critical service providers and setting proper risk tolerances. The PRA considers that these failures were particularly significant given the Firm's awareness of concerns relating to outsourcing (see paragraph 1.18 below).

1.8. The PRA has also considered those matters set out at Annexes A and B above.

1.9. Taking all of these factors into account, the PRA considers the seriousness of the conduct to be such that the appropriate Seriousness Percentage is 10%.

1.10. The Step 2 figure is therefore £1,144,400.

Step 3: Adjustment for any aggravating, mitigating or other relevant factors

1.11. Under the PRA's Penalty Policy, the PRA may increase or decrease the starting point figure to take account of any factors which may aggravate or mitigate the Breaches. Any such adjustment will normally be made by way of a percentage adjustment to the figure determined at Step 2[3].

[3] PRA Penalty Policy , paragraph 24

1.12. The PRA considers that the following factors are relevant:

(1) The Firm notified the PRA promptly of the IT Incident.

(2) Following the IT Incident, the Firm has undertaken significant remedial action to address the breaches (as detailed further at paragraphs 1.84 to 1.86 of Annex A to this Notice), and

(3) The Firm has cooperated with the FCA and PRA's joint investigation.

1.13. In the PRA's view these are the actions to be properly expected of an authorised firm in the circumstances.

1.14. The Firm's previous disciplinary history is also a relevant factor.

1.15. By way of the 2015 Final Notice, the PRA imposed a financial penalty of £1,278,165[4] on the Firm for breaches of Principle 3 of the Principles for Businesses during the period 18 December 2006 to 1 April 2014 for its failures (in summary) to:

(1) properly outsource important operational functions, specifically, the ATM finance function;

(2) manage the risks associated with, and oversee, the outsourced important operational functions; and

(3) have adequate systems and controls in place in relation to these outsourced services.

1.16. The 2015 Final Notice stated that the Firm had, upon discovering the transactions which ultimately became the subject of that PRA investigation, taken various actions which included "undertaking a Bank wide review of all outsourcing arrangements".

[4] The financial penalty would have been £1,825,950 were it not for the application of the 30% Stage 1 settlement discount.

1.17. The PRA considers that a number of specific failings which were the subject of the 2015 Final Notice are also present in this case. In particular:

(1) The Firm failed to carry out suitable due diligence adequately in respect of its outsourcing arrangements.[5]

(2) The Firm failed to enter into adequate contractual documentation with its outsourced service providers[6]; and

(3) The Firm failed to properly supervise the carrying out of the outsourced function(s) or that its outsourced service provider adequately managed the risks associated with the outsourcing.[7]

1.18. The 'Bank wide review' referred to at paragraph 1.16 above and in the 2015 Final Notice was conducted on a division-by-division basis at the request of senior management in April 2014. The PRA considers that the similarity between the failings in the 2015 Final Notice and this Notice raise serious doubts as to whether that review was adequately scoped, carried out to a satisfactory standard, overseen adequately with regular review points and, more generally, of the effectiveness of the Firm's remediation work during the early part of the Relevant Period.

1.19. The Firm had explicit notice of the PRA's concerns regarding the Firm's approach to outsourcing in advance of the 2015 Final Notice as a result of the PRA's investigation and a s. 166 Skilled Persons Review. It was also on notice that there were particular concerns relating to outsourcing within the Payment Services Division.

1.20. The PRA acknowledges that in 2015, the Firm had begun a root and branch overhaul of its Compliance function more widely and that the Firm viewed this as an important and necessary first step on its remediation journey. This work included instructing a leading audit firm to develop a comprehensive compliance monitoring plan and the appointment of a new Head of Compliance.

---

[5] 2015 Final Notice, paragraph 6
[6] 2015 Final Notice, paragraphs 5 and 7
[7] 2015 Final Notice, Annex B, paragraph 2.3

1.21. However, whilst acknowledging that some remedial steps were taken, actions taken by the Firm prior to the IT Incident were: (i) not comprehensive; (ii) implemented in an insufficiently timely manner; and (iii) did not consider the Firm's total exposure to outsourcing risk. This lack of adequate remediation, notwithstanding the steps that were taken, was evidenced when this risk crystallised in the IT Incident. Whilst some remedial action was in train, it did not adequately address the underlying issues until the end of the Relevant Period.

1.22. On balance, the PRA considers that the breaches reflected a repeat failing of the Firm's approach to outsourcing arrangements in circumstances where addressing such failings should have been a higher priority for the Firm. The PRA considers that repeat failings by a firm where it has previously taken enforcement action are particularly serious. For the avoidance of doubt, the PRA does not consider the Firm's repeat failing to have been deliberate or reckless.

1.23. As regards the Firm's disciplinary history, the PRA also notes that on 21 January 2019 the Office of Financial Sanctions Implementation (OFSI), part of HM Treasury, issued a monetary penalty of £5,000 in accordance with section 146 of the Policing and Crime Act 2017 against the Firm for a contravention of regulation 3 of the Egypt (Asset-Freezing) Regulations 2011 (S.I. 2011/887).

1.24. Considering the above factors taken as a whole, the PRA views the lack of timely, comprehensive and adequate remediation as significantly aggravating the severity of the breaches. The PRA considers that these factors justify an adjustment to the Step 2 figure of 40%.

1.25. The Step 3 figure is therefore £1,602,160.

Step 4: Adjustment for deterrence

1.26. Under the PRA's Penalty Policy, if the PRA considers the figure arrived at after Step 3 is insufficient to deter the firm that committed the breach, or others, from committing further or similar breaches, then the PRA may increase the penalty.

1.27. The PRA does not consider an adjustment for deterrence is necessary in this instance taking into account all the circumstances.

1.28. The Step 4 figure is, therefore £1,602,160.

Step 5: Application of any applicable reductions for early settlement or serious financial hardship

1.29. Pursuant to the PRA's Penalty Policy, if the PRA and the firm upon whom a financial penalty is to be imposed agree the amount of the financial penalty and any other appropriate settlement terms, the PRA's settlement policy provides that the amount of the penalty which would otherwise have been payable may be reduced.

1.30. The PRA and the Firm reached agreement at Stage 1 and so a 30% settlement discount applies to the Step 4 figure.

1.31. The Step 5 figure is therefore £1,121,512.

Conclusion

1.32. The PRA has therefore decided to impose **a financial penalty of £1,121,512** on the Firm for breaches of Fundamental Rules 2, 5 and 6 of the PRA Rulebook (as in force during the Relevant Period).

ANNEX D – PROCEDURAL MATTERS

1. DECISION MAKER

The settlement decision makers made the decision which gave rise to the obligation to give this Notice.

This Final Notice is given in accordance with section 390 of the Act.

2. MANNER AND TIME FOR PAYMENT

The Firm must pay the financial penalty in full to the PRA by no later than 12 June 2019, 14 days from the date of this Notice.

If all or any of the financial penalty is outstanding on the 13 June 2019, the day after the due date for payment, the PRA may recover the outstanding amount as a debt owed by the Firm and due to the PRA.

3. PUBLICITY

Sections 391(4), 391(6A) and 391(7) of the Act apply to the publication of information about the matter to which this Final Notice relates. Under these provisions the PRA must publish such information about the matter to which this Final Notice relates as the PRA considers appropriate. However, the PRA may not publish information if such information would, in the opinion of the PRA, be unfair to the persons with respect to whom the action was taken or prejudicial to the safety and soundness of PRA-authorised persons.

4. PRA CONTACTS

For more information concerning this matter generally, contact Jim Calveley, Deputy Head of Legal (direct line: 0203 461 8534, jim.calveley@bankofengland.co.uk), Eoghan McArdle, Legal Counsel (direct line: 0203 461 8877, eoghan.mcardle@bankofengland.co.uk) or Calum Macdonald, Legal Counsel (direct line: 0203 461 3153, calum.macdonald@bankofengland.co.uk) of the Enforcement and Litigation Division of the PRA.

APPENDIX 1 – DEFINITIONS

1. The definitions below are used in this Notice:

"the 2015 Final Notice" means the PRA's Final Notice to R. Raphael & Sons Plc dated 12 November 2015;

"the Act" means the Financial Services and Markets Act 2000 (as amended);

"BCP Questionnaire" means the *Third Party Business Continuity Management Questionnaire* which was appended to the Firm BCP and was designed to assess the adequacy of the business continuity plans of key outsource service providers;

"BIA" means Business Impact Analysis";

"BRATS" means the Firm's Board Risk Appetite and Tolerance Statement as in force during the Relevant Period;

"Card Agreement" means an agreement between the Firm and a Card Programme Manager setting out the contractual obligations of the Card Programme Manager;

"Card Payment Systems" means card payment systems such as Visa or MasterCard for which the Firm's responsibilities in relation to Card Programmes included registering the programme with a Card Payment System, obtaining a BIN from the relevant Card Payment System to enable payments to be authorised, and continually managing the settlement of payment transactions to the Card Payment System.

"Card Processor" means an outsourced service provider appointed by a Card Programme Manager who provided IT services (in particular, Payment Authorisation Services) in relation to a Card Programme;

"Card Programme" means a prepaid card or charge card programme operated by the Firm;

"Card Programme Manager" means an outsourced service provider appointed by the Firm who under a Card Agreement managed aspects of a Card Programme including procuring a Card Processor, customer relationship management, product marketing and ensuring availability of funds for daily settlement with the Card Payment Systems;

“Database Instance” means a set of memory structures that manages database files. A database is a set of physical files where data is stored. A Database Instance manages a single database’s stored data and serves the users of the database. Seven Database Instances at the Card Processor’s production data centre supported the Card Processor’s provision of IT services (including Payment Authorisation Services) to the impacted Card Programmes;

“DRATS” means the Firm’s Divisional Risk Appetite and Tolerance Statements as in force during the Relevant Period;

the “FCA” means the Financial Conduct Authority;

“Final Notice” or “Notice” means this notice, together with its Annexes and Appendices.

the “Firm” means R. Raphael & Sons plc;

the “Firm BCP” means the Firm’s central Business Continuity Plan as in force during the Relevant Period;

the “Initial IT Incident” means the incident which occurred on 18 April 2014 affecting the Card Processor’s systems supporting Payment Authorisation Services provided to the Firm;

the “IT Incident” means the incident which occurred on 24 December 2015 at the Card Processor’s production data centre and which resulted in the failure of the services it provided to the Firm for three Card Programmes;

“monitoring review” means an Outsource Monitoring Review of a Card Programme Manager in accordance with the Firm’s Outsource Monitoring Procedures

the “Outsourcing Policy” means the Firm’s General Outsourcing Policy as in force during the Relevant Period;

“Payment Authorisation Services” mean the real-time acceptance and processing of incoming authorisation requests from Card Payment Systems by a Card Processor;

the “PRA” means the Prudential Regulation Authority;

the “PRA Rulebook” means the Prudential Regulation Authority Rulebook;

the “PRA Penalty Policy” means ‘The Prudential Regulation Authority’s approach to enforcement: statutory statements of policy and procedure March 2019’ – Appendix 2 – Statement of the PRA’s policy on the imposition and amount of financial penalties under the Act;

the “PRA Settlement Policy” means ‘The Prudential Regulation Authority’s approach to enforcement: statutory statements of policy and procedure March 2019’ – Appendix 4 - Statement of the PRA’s settlement decision-making procedure and policy for the determination of the amount of penalties and the period of suspensions or restrictions in settled cases;

the “PSD” means the Firm’s Payments Services Division which is responsible for the Card Programmes;

the “PSD BCP” means the division-specific Business Continuity Plan for the Firm’s Payment Services Division;

the “PSD BIA” means the Business Impact Analysis carried out by the Firm’s Payment Services Division;

the “PSD DRATS” means the Payment Services Division’s Divisional Risk Appetite Statement as in force during the Relevant Period;

the “Relevant Period” means the period between 18 April 2014 and 31 December 2016 (inclusive); and

the “Tribunal” means the Upper Tribunal (Tax and Chancery Chamber).

APPENDIX 2 - RELEVANT STATUTORY AND REGULATORY PROVISIONS

RELEVANT STATUTORY OBJECTIVES

1.1. The PRA has a general objective, set out in section 2B of the Act, to promote the safety and soundness of PRA-authorised persons. The PRA seeks to advance this objective by seeking to ensure that the business of PRA-authorised firms is carried on in a way which avoids any adverse effect on the stability of the UK financial system.

1.2. Section 206 of the Act provides:

"If the appropriate regulator considers that an authorised person has contravened a relevant requirement imposed on the person, it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate."

1.3. The Firm is an authorised person for the purposes of section 206 of the Act. Relevant requirements imposed on authorised persons include rules imposed under the PRA Rulebook which are made under s. 137G of the Act.

RELEVANT REGULATORY PROVISIONS

1.4. References in this Final Notice to provisions in the PRA Rulebook and the PRA's Fundamental Rules are to the provisions as in force during the Relevant Period (or part thereof).

1.5. The PRA has eight Fundamental Rules which, from the 19 June 2014, applied to all PRA-authorised firms. These are high-level rules which collectively act as an expression of the PRA's general objective of promoting the safety and soundness of regulated firms.

1.6. Fundamental Rule 2 states that a firm must conduct its business with due skill, care and diligence.

1.7. Fundamental Rule 5 states that a firm must have effective risk strategies and risk management systems.

1.8. Fundamental Rule 6 states that a firm must organise and control its affairs responsibly and effectively.

1.9. Prior to the Fundamental Rules, the relevant high-level rules were the PRA's Principles for Businesses.

1.10. Principle 2 provided that a firm must conduct its business with due skill, care and diligence.

1.11. Principle 3 provided that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

1.12. In addition, SYSC 4.1.1 R (which was in force for the duration of the Relevant Period) requires a firm to have effective processes to identify, manage, monitor and report the risks it is or might be exposed to.

1.13. SYSC 8.1.1.R (which again was in force for the duration of the Relevant Period) required that a firm must:

> "*(1) when relying on a third party for the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary services … on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk;*
>
> *(2) not undertake the outsourcing of important operational functions in such a way as to impair materially:*
>
> *(a) the quality of its internal control; and*
>
> *(b) the ability of the appropriate regulator to monitor the firm's compliance with all obligations under the regulatory system and, if different, of a competent authority to monitor the firm's compliance with all obligations under MiFID.*"

1.14. Furthermore, the PRA Rulebook, from 2 April 2015 contained detailed rules relating to the outsourcing of services by a firm (the Outsourcing Rules).

1.15. PRA Outsourcing Rule 2.1 states:

"*A firm must:*

a. *when relying on a third party for the performance of operational functions which are critical for the performance of relevant services and activities on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk;*

b. *not undertake the outsourcing of important operational functions in such a way as to impair materially:*
   a. *the quality of its internal control; and*
   b. *the ability of the PRA to monitor the firm's compliance with all obligations under the regulatory system and, if different, of a competent authority to monitor the firm's compliance with all obligations under MiFID."*

1.16. Outsourcing Rule 2.2 states:

"*For the purposes of this Part an operational function is regarded as critical or important if a defect or failure in its performance would materially impair the continuing compliance of a firm with the conditions and obligations of its authorisation or its other obligations under the regulatory system, or its financial performance, or the soundness or the continuity of its relevant services and activities*."

1.17. Outsourcing Rule 2.4 states:

"If a firm outsources critical or important operational functions or any relevant services and activities, it remains fully responsible for discharging all of its obligations under the regulatory system and must comply, in particular, with the following conditions:

(1) the outsourcing must not result in the delegation by senior personnel of their responsibility;

(2) the relationship and obligations of the firm towards its clients under the regulatory system must not be altered;

(3) the conditions with which the firm must comply in order to be authorised, and to remain so, must not be undermined;

(4) none of the other conditions subject to which the firm's authorisation was granted must be removed or modified."

1.18. Outsourcing Rule 2.5 states:

"A firm must exercise due skill and care and diligence when entering into, managing or terminating any arrangement for the outsourcing to a service provider of critical or important operational functions or of any relevant services and activities."

1.19. Outsourcing Rule 2.6 states:

"A firm must in particular take the necessary steps to ensure that the following conditions are satisfied:

(1) the service provider must have the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally;

(2) the service provider must carry out the outsourced services effectively, and to this end the firm must establish methods for assessing the standard of performance of the service provider;

(3) the service provider must properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing;

(4) appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements;

(5) the firm must retain the necessary expertise to supervise the outsourced functions effectively and to manage the risks associated with the outsourcing, and must supervise those functions and manage those risks;

(6) the service provider must disclose to the firm any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements;

(7) the firm must be able to terminate the arrangement for the outsourcing where necessary without detriment to the continuity and quality of its provision of services to clients;

(8) the service provider must co-operate with the PRA and any other relevant competent authority in connection with the outsourced activities;

(9) the firm, its auditors, the PRA and any other relevant competent authority must have effective access to data related to the outsourced activities, as

well as to the business premises of the service provider; and the PRA and any other relevant competent authority must be able to exercise those rights of access;

(10) the service provider must protect any confidential information relating to the firm and its clients;

(11) the firm and the service provider must establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities where that is necessary having regard to the function, service or activity that has been outsourced.

1.20. Outsourcing Rule 2.7 states*:*

"A firm must ensure that the respective rights and obligations of the firm and of the service provider are clearly allocated and set out in a written agreement".

RELEVANT STATUTORY POLICY

Approach to the supervision of banks

1.21. *The Prudential Regulation Authority's Approach to Banking Supervision, June 2014* (as updated in October 2018) sets out how the PRA carries out its role in respect of deposit-takers and designated investment firms. One of the purposes of the document is to communicate to regulated firms what the PRA expects of them, and what they can expect from the PRA in the course of supervision.

Approach to enforcement

1.22. *The Prudential Regulation Authority's approach to enforcement: statutory statements of* policy *and procedure*, *April 2013* (as updated in March 2019) sets out the PRA's approach to exercising its main enforcement powers under the Act.

1.23. In particular, The PRA's approach to the imposition of penalties is outlined at Annex 2 *Statement of the PRA's policy on the imposition and amount of financial penalties under the Act*; and the PRA's approach to settlement is outlined at Annex 4 - *Statement of the PRA's settlement decision-making procedure and policy for the determination of the amount of penalties and the period of suspensions or restrictions in settled cases*.