FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

FINAL NOTICE

To: **R. Raphael & Sons plc**

Reference Number: **161302**

Address: **19-21 Shaftesbury Avenue, London, W1D 7ED**

Date: **29 May 2019**

1. ACTION

1.1. For the reasons given in this Final Notice, the Authority hereby imposes on R. Raphael & Sons plc ("Raphaels" or "the Firm") a financial penalty of £775,100 pursuant to section 206 of the Act.

1.2 Raphaels agreed to resolve this matter and qualified for a 30% (Stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £1,107,414 on the Firm.

2. SUMMARY OF REASONS

2.1. The Firm is an independent bank involved in the provision of banking and related financial services. The Firm is regulated by the Authority 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 approximately 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 outsource 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. During the early hours of 24 December 2015, a technology incident occurred at a Card Processor resulting in the complete failure of all services it provided to the Firm for three Card Programmes (the "IT Incident").

2.5. As a result of the IT Incident, which lasted over eight hours, 3,367 of the Firm's customers were unable to use their prepaid cards and charge cards during this time on Christmas Eve. In total, the Card Processor could not authorise 5,356 customer card transactions attempted at point of sale terminals, ATM machines and online (worth an aggregated value of £558,400). The IT Incident also prevented customers from viewing their card balances online.

2.6. The cause and duration of the IT Incident reflected shortcomings in Raphaels understanding of the business continuity and disaster recovery arrangements of the Card Processor. The Firm had no adequate processes for capturing and assessing information regarding these arrangements, particularly how they would support the continued operation of the Card Programmes during a disruptive event.

2.7. The absence of any adequate processes for capturing and assessing information about the Card Processor's business continuity and disaster recovery arrangements exposed the Firm and its customers to a serious risk of harm. As Raphaels was unaware of the risk, it could take no steps to manage or mitigate it. On 24 December 2015, this risk crystallised.

2.8. The Firm's specific failings in relation to the IT Incident resulted from deeper flaws in its governance of critical outsourced services and outsource service providers

and a failure to take appropriate action when a similar IT failing occurred 20 months prior to the IT Incident. In particular:

(1) Raphaels' over-arching statements of its risk appetite and tolerance failed to adequately articulate the appetite for and tolerance levels in relation to the Firm's use of outsourcing and, in particular, the outsourcing of critical services. This failing prevented it from determining when its use of critical outsourcing exceeded the level of risk it was willing and able to accept;

(2) Raphaels' contractual agreements with Card Programme Managers failed to include appropriate service level agreements governing the provision of critical outsourced services;

(3) Raphaels had no process in place for identifying its critical outsourced services and functions;

(4) Raphaels' business continuity and disaster recovery planning focussed only on services performed directly by the Firm notwithstanding:

- its heavy reliance on outsourced services and the interdependence between those services and the services it performed; and

- its ultimate responsibility for the effective provision of outsourced services.

(5) Raphaels' initial due diligence on Card Programme Managers and Card Processors did not involve adequate consideration of business continuity arrangements, and its ongoing monitoring of such arrangements was flawed; and

(6) Raphaels failed to respond appropriately when an 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, it 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.

2.9. These flaws meant that, during the relevant period, the Firm was not in a position properly to assess or monitor the business continuity and disaster recovery arrangements for any of the critical services outsourced under its Card Programmes, exposing it and its customers to risk.

2.10. The Authority hereby imposes on Raphaels a financial penalty of £775,100 pursuant to section 206 of the Act for failing to comply with Principles 2 and 3, as well as the applicable provisions of Chapter 8 of the Authority's Senior Management Arrangements, Systems and Controls sourcebook ("SYSC 8").

2.11. The Authority has investigated the Firm's arrangements in respect of outsourced services provided on behalf of the PSD and in particular in respect of the business continuity and disaster recovery provision made by outsource service providers. For the reasons explained in this Final Notice, the Authority 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 Final Notice is from 18 April 2014 to 31 December 2016.

3. DEFINITIONS

3.1. The definitions below are used in this Final Notice:

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

"the Authority" means the body corporate previously known as the Financial Services Authority and renamed on 1 April 2013 as the Financial Conduct Authority;

"BIN" means Bank Identification Number designated by the first few digits of a payment card issued by a financial institution. Among other things, the number is used to verify payment transactions made via a particular Card Payment System;

"Card Agreement" means the formal contract between the Firm and a Card Programme Manager setting out the obligations of each party;

"Card Payment System" means card systems such as Visa or MasterCard responsible, amongst other things, for routing card payment authorisation and settlement requests between merchant acquirers and issuing banks (e.g. Raphaels);

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

"Card Programme Manager" means an outsource service provider appointed by the Firm under a Card Agreement to manage aspects of a Card Programme including procuring a Card Processor, customer relationship management, product marketing and ensuring sufficient funds are held in the accounts supporting the Card Programme for daily settlement with the Card Payment Systems;

"Card Processor" means an outsource service provider appointed by a Card Programme Manager and formally approved by the Firm to predominantly provide IT services (including Payment Authorisation Services) in relation to a Card Programme;

"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;

"Executive Committee" means the Executive Committee of R. Raphael & Sons Plc;

"Handbook" means the Financial Conduct Authority Handbook;

"High Availability" means a quality of a system or component that assures a high level of operational performance for a given period of time;

"Joint Operating Manual" means a manual agreed between the Firm and a Card Programme Manager describing, among other things, the operational responsibilities of each party in relation to a Card Programme;

"Maximum Tolerable Downtime" and "MTD" means the time after which an organisation's viability could be irrevocably threatened if product and service delivery cannot be resumed;

"outsourcing" means an arrangement of any form between a firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the firm itself;

"Outsourcing Policy" means the Firm's General Outsourcing Policy;

"outsource service provider" means a third party which performs outsourcing functions and services on behalf of a firm;

"PRA" means the Prudential Regulation Authority;

"PSD" means the Firm's Payment Services Division;

"Payment Authorisation Services" means the real-time acceptance and processing of incoming payment authorisation requests performed by a Card Processor;

"Raphaels" or "the Firm" means R. Raphael & Sons Plc;

"Recovery Time Objective" and "RTO" means the timeframe for restoring services to a level where an organisation's reputation or its financial condition is not too seriously affected; and

"the Tribunal" means the Upper Tribunal (Tax and Chancery Chamber).

4. FACTS AND MATTERS

Outsourcing – Regulatory Expectations

4.1. When carrying on its regulated activities, a firm may choose to outsource certain functions and services to third parties. Nevertheless, firms retain full accountability for discharging their regulatory obligations and cannot delegate them to other parties.

4.2. During the relevant period, the Firm was required, when relying on a third party for the performance of operational functions which were critical for the performance of regulated activities on a continuous and satisfactory basis, to ensure that it took reasonable steps to avoid undue additional operational risk. For these purposes, an operational function is regarded as critical if (among other things) a defect or failure in its performance would materially impair the soundness or the continuity of its relevant services and activities. Therefore, to determine whether a particular service or function was critical, the Firm was required to consider the impact on its regulated activities if that service or function was subject to disruption.

Background

4.3. Raphaels, one of the oldest UK independent retail banks, is authorised by the PRA and jointly regulated by the Authority and PRA. The Firm has a number of business divisions including Payment Services, Lending and Savings.

4.4. Raphaels is a principal member of the Visa and Mastercard Card Payment Systems and, through such membership, provides sponsorship for the issuance of prepaid cards and charge cards.

4.5. Raphaels' 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, Raphaels receives funds 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.

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

Card Programmes

4.7. Raphaels 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.

4.8. Raphaels' responsibilities in relation to Card Programmes include registering the programme with the Card Payment System, obtaining a Bank Identification Number ("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. For all relevant Card Programmes, the Firm has a direct legal relationship with, and regulatory responsibility for, the cardholder.

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

4.10. A Card Programme Manager's obligations are set out in a formal contract with the Firm ("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.

4.11. Provided the Firm has approved in writing the choice of Card Processor, the Card Programme Manager and the Card Processor enter into a contract regarding the provision of services by the Card Processor. The services provided by a Card Processor are detailed in both its contract with the Card Programme Manager and the Card Agreement. They are predominantly IT services which include daily transaction reporting, fraud management monitoring and Payment Authorisation Services.

4.12. The Firm enters into a "Compliance Agreement" with each Card Processor, principally to ensure that the Firm can take control of a Card Programme should the relevant Card Programme Manager become unresponsive. In particular, the Compliance Agreement enables the Firm to instruct the Card Processor to decline a specific transaction or set of transactions.

Critical Outsourcing - Appetite and Identification

Outsourcing Risk Appetite

4.13. Whether considered individually or collectively, none of the procedure and policy documents described in this Final Notice provided a process for identifying the Firm's "critical" outsourced services and functions. None of these documents established an appropriate critical outsourcing risk appetite. As a result, the Firm was unable to determine when its use of critical outsourcing exceeded the level of risk it was willing and able to accept.

4.14. The Firm's approach to managing risk is governed by its Risk Management Policies and Procedures ("RMPP"). A fundamental purpose of the RMPP is to assist staff members with identifying and assessing risks. The RMPP identifies Raphaels' Board as the ultimate decision-making body with responsibility for determining the Firm's overall risk appetite and tolerance levels.

4.15. The Board articulates the risks and tolerance levels the Firm is willing to accept through its Board Risk Appetite and Tolerance Statement ("BRATS"), 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.

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

4.17. At the time of the IT Incident, the RMPP explicitly identified "Outsourcing" as one of four principal risks for which the Firm needed to hold capital. However,

outsourcing risk was not specifically identified in the BRATS. The Firm's approach was to articulate outsourcing risk as a category of operational risk. However, the Board's description of operational risk within the BRATS did not explicitly refer to risks of outsourcing (including critical outsourcing) nor the use of outsource service providers. Instead, outsourcing risk and the tolerance levels accepted by the Firm for specific outsourcing risks were impliedly captured by general references to preventing "operational losses" and "compliance failures".

4.18. The 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).

4.19. The BRATS 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 related solely to the Firm's internal IT processes and had no relation to the business continuity and disaster recovery plans of its outsourced service providers.

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

4.21. 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

4.22. The Firm has had a documented "General Outsourcing Policy" in place since January 2012 (the "Outsourcing Policy"). 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. The policy was approved by both the Board and Executive Committee.

4.23. The Outsourcing Policy listed the general outsourcing requirements under SYSC 8, 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.

4.24. 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".

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

4.26. The Outsourcing Policy referred to specific intra-group outsourced functions and services (i.e. functions and services outsourced to other entities in 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.

4.27. 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 all critical outsourced services required to operate a Card Programme.

4.28. The separate contracts agreed between the Card Programme Manager and the Card Processor did, however, contain service level agreements relating to the provision of certain critical outsourced services. However, Raphaels 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

4.29. All Card Agreements in force at the time of the IT Incident required both the Firm and the relevant Card Programme Manager to each 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".

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

4.31. 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.

4.32. 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 replicated the production data centre;

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

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

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

Raphaels' Business Continuity Plans

4.33. At the time of the IT incident, Raphaels had in place a central business continuity plan (the "Raphaels BCP"). The Raphaels 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.

4.34. The Raphaels' BCP required risk assessments for each of its "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. The BIA was intended to identify and document the key risks to business continuity within the division. As part of formulating the BIA, each division was required to specify appropriate Recovery Time Objectives (RTOs) and Maximum Tolerable Downtimes (MTDs) for its "critical functions". A Recovery Time Objective is the timeframe for restoring services to a level where the Firm's reputation or its financial condition is not too seriously affected. Maximum Tolerable Downtime is the time after which the Firm's viability could be irrevocably threatened if product and service delivery cannot be resumed.

4.35. The Raphaels BCP required each of its 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 outsource service provider that an "up-to-date, fully documented and tested" business continuity plan was in place. However, the Raphaels 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 the Firm to approve the adequacy of those plans or ensure they were linked to the PSD's RTO or MTD figures.

The Third Party Business Continuity Management Questionnaire

4.36. The Raphaels 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. However, the Raphaels BCP noted that not all suppliers and outsourced providers would be willing to complete the BCP Questionnaire. In those circumstances, how a division (e.g. the PSD) obtained the information was stated in the Raphaels BCP to be at the discretion of management.

4.37. The BCP Questionnaire did not seek any details of the relevant arrangements of sub-contractors (e.g. Card Processors) providing critical services to the Firm, and sub-contractors were not expected to respond to the questionnaire. 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.

4.38. Raphaels did not provide any guidance or training for those reviewing responses to the BCP Questionnaire and any supporting evidence provided. Moreover, despite the heavy reliance on 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 BCP Questionnaire.

4.39. The BCP Questionnaire contained important questions concerning business continuity and recovery for outsource services. However, it was not completed by all directly contracting outsource 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

4.40. The PSD maintained a separate 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 Raphaels BCP, the PSD BCP included a BIA assessment (including relevant RTO and MTD levels)

of its key systems and functions. However, this only considered internal systems and functions, and did not include consideration of any outsourced functions.

4.41. 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 this was "covered in part" by the PSD requiring all Card Programme Managers to have a BCP open for inspection and less than one year old; the Joint Operating Manuals detailing operating procedures; and by using major blue-chip technology providers for its major programmes.

4.42. Neither the Raphaels BCP nor 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 any impact that disruption to those services could have on Raphaels and its customers.

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

4.44. 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.

4.45. 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, Raphaels undertook no assessment of the impact which disruption to these services or functions might have on it and its customers. Furthermore, it undertook no criticality assessment of the relative importance of

these services and functions (including the assignment of appropriate RTO and MTD levels) to the business of the PSD.

Assessment of outsourced service business continuity and disaster recovery arrangements

i. Initial Due Diligence

4.46. 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. Among 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.

4.47. 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 assessed two of the three Card Programme Managers' business continuity plans. However, both reviews were high-level, providing little indication of which continuity and recovery arrangements were assessed or how they satisfied the Firm and PSD's requirements.

4.48. For the third Card Programme Manager, there was no initial review of business continuity or recovery arrangements. Had it undertaken such a review, the Firm would have identified that the business continuity plan contained no "time frame for recovering critical business functions" as required by the relevant Card Agreement.

4.49. 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 to request 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 there was no formal requirement to initially assess a Card Processor's business continuity and disaster recovery arrangements.

4.50. 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 which

was later subject to the IT Incident. 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 Authority has seen no evidence indicating that this concern was followed up prior to the IT Incident.

ii. Ongoing Monitoring

4.51. Once a Card Programme had 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 to which it had sub-contracted services.

4.52. The annual form was not sent to, nor did it mention, Card Processors. Instead, Raphaels relied on its Card Programme Managers to conduct ongoing due diligence of Card Processor(s). 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.

4.53. The PSD also conducted outsource monitoring reviews ("monitoring reviews") of its Card Programme Managers in accordance with its "Outsource Monitoring Procedures".

4.54. The monitoring reviews were intended, 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.

4.55. 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. Accordingly, the PSD carried out an initial risk assessment of the Card Programme Managers to determine when each review

would take place. The assessment considered the products, processes, jurisdiction of operation and past performance of the Card Programme Manager.

4.56. However, the assessment did not seek to identify whether any of the services provided by or on behalf of the Card Programme Manager constituted critical outsourcing under SYSC 8. Moreover, resourcing constraints within the PSD prevented certain Card Programme Managers from receiving a monitoring review as scheduled.

4.57. Consequently, the PSD could not ensure that all Card Programme Managers providing or otherwise responsible for critical outsourced services, received a timely monitoring review.

4.58. 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 for how to assess business continuity plans and their test results. This is because the PSD had no such guidance in place.

4.59. 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 Firm's requirements. 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.

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

each visit identified that the Card Programme Managers were not adequately monitoring the activities of the Card Processor.

4.61. There was no review of the Card Programme Managers' business continuity plans in the year prior to the IT Incident. Consequently, the Firm was not aware that two of the Card Programme Managers' plans had not been updated since 2012 and 2013 respectively, contravening the requirement that "BCPs should be less than 1 year old".

4.62. The Card Programme Managers were contractually required to ensure that the Card Processor maintained a business continuity plan (although there was no requirement as to the form this should take or what it should contain). The Firm also relied on the 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

4.63. 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.

4.64. 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.

4.65. Between 9 June to 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.

4.66. 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.

The Initial IT Incident

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

4.68. 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 (the same two Card Programmes were also impacted by the IT Incident).

4.69. The Card Processor reported that the Initial IT Incident was an "unexpected eventuality" and that it had been addressed. However, Raphaels 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. Moreover, the Firm did not seek to ascertain the impact of the incident on its 57 customers.

4.70. 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.

4.71. 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.

4.72. In July 2014, the Authority published "*Considerations for firms thinking of using third-party technology (off-the-shelf) banking solutions*". This publication raised concerns about firms' arrangements for outsourced service resilience, disaster recovery and business continuity planning, including the need for alignment between such arrangements.

The IT Incident

Overview

4.73. During the early hours of 24 December 2015, a technology 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 affected by the IT Incident included the Card Processor's provision of Payment Authorisation Services.

4.74. 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.

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

4.76. 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.

4.77. 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 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 "standby system" in order to restore Payment Authorisation Services. This task took over seven hours to complete, which breached the Firm's objective that Payment Authorisation Services should recover within four hours.

4.78. Raphaels 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 when only those two Database Instances had malfunctioned.

4.79. As a result of the Initial IT Incident in 2014, the Firm was or should have been aware that even a partial disruption to the Card Processor's high availability setup could impact the supply of Payment Authorisation Services. The Firm was also already on notice that the Card Processor's business continuity plan would not be invoked for day-to-day system failure.

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

4.81. 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 04:22am (GMT) but the Firm was not made aware of the disruption and consequent impact on its customers before 09:00am (GMT). Had the Firm been alerted earlier, it could have taken steps to mitigate the impact of the IT Incident on customers sooner.

4.82. 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.

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

4.84. 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 incident. These communications included complaints from customers who were unable to withdraw money, pay their bills or use their prepaid cards for Christmas shopping.

4.85. At 09:25am, following discussions with the Firm, the Card Programme Manager placed a notification on its website explaining the incident had occurred and was preventing customers from using their cards. The notification stated that a customer services team was in place to handle customer calls.

4.86. Customers who contacted customer services were offered the option to access up to £250 via an alternative bank account. To facilitate this, the Card Programme Manager asked the Firm to release funds from its own account with the Firm. The Card Programme Manager also sent text messages to customers to update them on the disruption. Following resolution of the incident, the Card Programme Manager sent a further text message to customers confirming that services had been restored.

4.87. These were impromptu measures initiated by the Card Programme Manager and approved by Raphaels. They were not part of any formal business continuity or disaster recovery plan.

Actions taken by Raphaels following the IT Incident

4.88. Immediately following the IT Incident, the Firm requested the Card Processor to 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.

4.89. However, the Firm did not seek to investigate whether customers of the three impacted Card Programmes suffered any detriment. Consequently, no redress was offered to those customers notwithstanding any loss, inconvenience or distress they experienced due to the IT Incident.

4.90. In early 2016, the Firm 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 Authority's Handbook and the PRA Rulebook. The assessments focused on outsourcing by the PSD.

4.91. 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 external firm identified gaps and weaknesses in the PSD's "contingency and business continuity planning" in relation to outsourced services.

4.92. 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:

i. identifying outsourcing risk as a standalone risk in the BRATS;

ii. the introduction of new end-to-end outsourcing procedures for managing the risks to its critical outsourced services;

iii. revised due diligence procedures for Card Programme Managers to ensure a more comprehensive and holistic assessment is undertaken;

iv. enhancements to the assessment and management of the business continuity plans for critical outsource service providers; and

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

4.93. In April 2017, the Authority required Raphaels to appoint a Skilled Person to assess whether the Firm was compliant with the Authority'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 Raphaels' design and execution of its outsourcing systems and controls broadly enabled the Firm to comply with applicable regulations.

5. FAILINGS

5.1. The regulatory provisions relevant to this Final Notice are referred to in Annex A.

5.2. Based on the facts and matters above, the Authority considers that Raphaels breached Principle 3 and associated provisions of SYSC 8, and Principle 2, as explained below.

Breach of Principle 3 and SYSC 8

5.3. Principle 3 requires that a firm take reasonable steps to ensure that it has organised its affairs responsibly and effectively, with adequate risk management systems. During the relevant period, SYSC 8.1.1R required Raphaels, when

relying on a third party for the performance of functions which were critical for the performance of regulated activities on a continuous and satisfactory basis, to ensure that it took reasonable steps to avoid undue additional operational risk.

5.4. During the relevant period, Raphaels breached Principle 3 and SYSC 8.1.1R because its systems and controls failed to enable it properly to identify when it was relying on outsourcers for the performance of functions that were critical for the performance of its regulated activities (in particular, the provision of e-money) on a continuous and satisfactory basis. It was unable to ensure it took reasonable steps to avoid undue additional operational risk, and its risk management systems were therefore inadequate. The facts and matters that caused these failings were as follows:

(1) Raphaels' BRATS and the PSD DRATS failed to adequately articulate the appetite for and tolerance levels in relation to the Firm's use of outsourcing and, in particular, the outsourcing of critical services. The absence of a clearly defined outsourcing risk appetite meant the Firm could not determine when its use of 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) Raphaels' 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 Raphaels' own requirements.

(3) The Raphaels' BCP and PSD BCP did not address business continuity in relation to outsourced services. This meant that there was no business impact analysis 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 on how to assess such information.

(4) Raphaels' 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 not even a policy on what information about these should be obtained from Card Processors.

(5) Raphaels did not subject Card Processors to operational reviews, monitoring reviews or require them to complete annual due diligence forms. The Firm was therefore almost entirely dependent 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, 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.

(6) The Firm's monitoring arrangements for Card Programme Managers did not require it to give adequate consideration to business continuity matters, and no adequate guidance was provided to the Firm's staff for any ongoing monitoring review which did consider such matters. As a result, the business continuity plans of Card Programme Managers were not reviewed against clear requirements of the Firm, creating a risk that they would not align with the Firm's requirements. Raphaels' risk-based assessment of when monitoring reviews should take place took no account of the criticality of the outsourced services. Resourcing constraints meant that it failed to conduct the reviews its flawed assessment process had identified it should on a timely basis.

(7) Raphaels' "operational reviews" made inadequate inquiry into the business continuity arrangements of Card Programme Managers and took inadequate account of arrangements at the Card Processor.

5.5. Raphaels' failings created a risk that those outsourcers carrying out services on its behalf that were critical to the PSD's regulated activities would not have adequate arrangements in place to deal with interruptions to their business. That risk crystallised when the IT Incident occurred. However, the failings were of a wider significance, because the risk applied across all of the Card Programme Managers and Card Processors on which the PSD relied.

Breach of Principle 2

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

5.7. Raphaels breached Principle 2 by failing to take proper steps in response to the Initial IT Incident to investigate its underlying cause and the impact on its customers. Furthermore, the Firm 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 Raphaels taken such steps, it may have identified, and remedied, the problems with the Card Processor's arrangements that contributed to the impact of the IT Incident.

6. SANCTION

Financial penalty

6.1. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms. The Authority considers it appropriate to consider the penalty for all the breaches as a whole.

Step 1: disgorgement

6.2. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

6.3. The Authority has not identified any financial benefit that Raphaels derived directly from its breach.

6.4. Step 1 is therefore £0.

Step 2: the seriousness of the breach

6.5. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.6. The Authority considers that the revenue generated by Raphaels is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of Raphaels' relevant revenue. Raphaels' relevant revenue is the revenue derived by Raphaels during the period 18 April 2014 to 31 December 2016 in respect of all Card Programmes. The Authority considers Raphaels' relevant revenue for this period to be £9,629,689.

6.7. In deciding on the percentage of the relevant revenue that forms the basis of the step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach; the more serious the breach, the higher the level. For penalties imposed on firms there are the following five levels:

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

6.8. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly. The factors that the Authority considers to be relevant to the Firm's breaches are set out below.

Impact of the breach

6.9. All of the Firm's card users were exposed to the risk created by the breach.

6.10. The IT Incident lasted for over eight hours and resulted in 3,367 of Raphaels' customers (many of whom had little or no recourse to alternative funds) being unable to use their pre-paid or charge cards when they attempted to. 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.

6.11. Although the Firm has not identified any financial loss, the IT Incident caused distress and inconvenience to many customers. 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, including customers complaining that they had not been able to withdraw money, pay their bills or make purchases. The IT Incident occurred on Christmas Eve thereby compounding the distress suffered by those customers.

6.12. The most substantial Card Programme that was affected by the IT Incident was provided primarily to seasonal workers who depended on their cards to receive their wages, and were likely to include vulnerable customers.

Nature of the breach

6.13. The breach revealed serious systemic weaknesses in the Firm's governance of critical outsourced services and outsource service providers.

Level of seriousness

6.14. DEPP 6.5A.2G(11) lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factor to be relevant:

a) The breach revealed serious systemic weaknesses in the Firm's governance of critical outsourced services and outsource service providers.

6.15. DEPP 6.5A.2G(12) lists factors likely to be considered 'level 1, 2 or 3 factors'. Of these, the Authority considers the following factors to be relevant:

a) Little, or no, profits were made or losses avoided as a result of the breach, either directly or indirectly;

b) there was no, or limited, actual or potential effect on the orderliness of, or confidence in, markets as a result of the breach; and

c) The breach was committed negligently or inadvertently.

6.16. Taking all of these factors into account, the Authority considers the seriousness of the breach to be level 3 and so the Step 2 figure is 10% of £9,629,689.

6.17. Step 2 is therefore £962,969.

Step 3: mitigating and aggravating factors

6.18. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.

6.19. The Authority considers that the following factors aggravate the breach:

a) Raphaels should have been on notice of the importance of properly overseeing its critical outsourcing arrangements. On 12 November 2015, the PRA imposed a financial penalty of £1,278,165 on the Firm for failing to, among other things, manage and oversee the risks associated with outsourcing important operational functions between 18 December 2006 and 1 April 2014.

b) In July 2014, prior to the IT Incident, the Authority published "*Considerations for firms thinking of using third-party technology (off-the-shelf) banking solutions"*. This publication raised relevant concerns around firms' arrangements for outsourced service resilience, disaster recovery and business continuity planning (including the need for alignment between such arrangements).

c) Although Raphaels helped facilitate access to alternate funds, during the IT Incident this was only communicated to customers who called the customer services team. Raphaels did not seek to investigate whether customers of the three impacted Card Programmes suffered any detriment as a result of the IT Incident. All customers who had a transaction declined or who were otherwise unable to access their funds suffered inconvenience. Many are likely to have suffered distress, and some may have suffered financially. As noted above, the affected customers are likely to have included vulnerable customers. Such customers are more likely to be adversely affected than others, at the same time as being less likely to be able to take action to seek redress. Nevertheless, Raphaels took no steps to offer redress to those customers notwithstanding any loss, inconvenience or distress they experienced.

6.20. Having taken into account these aggravating factors, the Authority considers that the Step 2 figure should be increased by 15%.

6.21. The Step 3 figure is therefore £1,107,414.

Step 4: adjustment for deterrence

6.22. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.23. The Authority considers that the Step 3 figure of £1,107,414 represents a sufficient deterrent to Raphaels and others, and so has not increased the penalty at Step 4.

6.24. The figure at Step 4 therefore remains at £1,107,414.

Step 5: settlement discount

6.25. Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement.

6.26. The Authority and Raphaels reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure. The Step 5 figure is therefore £775,100. It is the Authority's usual practice to round down the final penalty figure to the nearest £100.

Penalty

6.27. The Authority hereby imposes a total financial penalty of £775,100 on Raphaels for breaching Principles 2 and 3 and associated rules of SYSC 8.

7. PROCEDURAL MATTERS

7.1. This Final Notice is given to Raphaels under and in accordance with section 390 of the Act.

7.2. The following statutory rights are important.

Decision maker

7.3. The decision which gave rise to the obligation to give this Final Notice was made by the Settlement Decision Makers.

Manner of and time for payment

7.4. The financial penalty must be paid in full by Raphaels to the Authority by no later than 12 June 2019.

If the financial penalty is not paid

7.5. If all or any of the financial penalty is outstanding on 13 June 2019, the Authority may recover the outstanding amount as a debt owed by Raphaels and due to the Authority.

Publicity

7.6. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

Authority contacts

7.7. For more information concerning this matter generally, contact Lisa Ablett at the Authority (direct line: 020 7066 9886 / email: Lisa.Ablett@fca.org.uk) or Joseph Nourse at the Authority (direct line: 020 7066 5512 / email: Joseph.Nourse@fca.org.uk).

Anthony Monaghan

Head of Department
Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A

RELEVANT STATUTORY AND REGULATORY PROVISIONS

1.1. The Authority's statutory objectives, set out in section 1B(3) of the Act, include the consumer protection objective.

1.2. Section 206(1) of the Act provides:

"If the Authority considers that an authorised person has contravened a requirement imposed on him by or under this Act… it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate."

RELEVANT REGULATORY PROVISIONS

Principles for Businesses

1.3. The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority's Handbook. They derive their authority from the Authority's rule-making powers set out in the Act. The relevant Principles are as follows.

1.4. Principle 2 provides:

"A firm must conduct its business with due skill, care and diligence".

Principle 3 provides:

"A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."

SYSC 8 (as in force during the Relevant Period)

1.5. SYSC 8.1.1R states:

"*A common platform 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 (in this chapter "relevant services and activities") 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."

1.6. SYSC 8.1.4R states:

"For the purposes of this chapter 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 common platform 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."

DEPP

1.7. Chapter 6 of DEPP, which forms part of the Authority's Handbook, sets out the Authority's statement of policy with respect to the imposition and amount of financial penalties under the Act.

The Enforcement Guide

1.8. The Enforcement Guide sets out the Authority's approach to exercising its main enforcement powers under the Act.

1.9. Chapter 7 of the Enforcement Guide sets out the Authority's approach to exercising its power to impose a financial a penalty.