
FINAL NOTICE

To: Card Protection Plan Limited

FSA

Reference

Number: 311489

Date: 14 November 2012

1. ACTION

- 1.1. For the reasons given in this notice, the FSA hereby imposes on CPP a financial penalty of £10.5 million.
- 1.2. CPP agreed to settle at an early stage of the FSA's investigation. CPP therefore qualified for a 30% Stage 1 discount under the FSA's executive settlement procedures. Were it not for this discount, the FSA would have imposed a financial penalty of £15 million on CPP.

Summary of Reasons

- 1.3. The FSA takes this action because, when CPP sold Card Protection and Identity Protection to customers, it breached Principles 6 and 7 (for the period January 2005 to March 2011) and Principle 3 (for the period June 2008 to March 2011).

Breach of Principle 7

- 1.4. From January 2005 to March 2011, CPP failed to communicate with customers in a way that was clear, fair and not misleading because:
 - (1) it sold its Card Protection product by emphasising to customers that one aspect of the product would be that they would benefit from up to £50,000 or £100,000 (the figure varied over time) worth of insurance cover when in fact customers did not need this cover;
 - (2) in relation to other aspects of the Card Protection insurance cover, it failed to explain the very limited circumstances in which customers would need the cover; and
 - (3) in relation to its Identity Protection product it overstated the risks and repercussions of identity theft in its sales and its Customer Documentation.

Breach of Principle 6

- 1.5. From January 2005 to March 2011, CPP's sales process promoted an excessive focus on sales, revenue and commercial objectives at the expense of treating customers fairly in that it:
- (1) encouraged sales agents to be overly persistent in persuading potential customers of both products to purchase them even after the customers had made it clear that they did not wish to buy them;
 - (2) gave its sales agents targets for successfully dissuading customers who contacted CPP to cancel their policies. This created a risk of sales agents using inappropriate objection handling techniques to discourage customers when they tried to cancel their policies;
 - (3) did not contain sufficient safeguards to prevent sales agents inappropriately seeking to persuade customers to buy the products on the basis that customers could cancel them during the cooling-off period;
 - (4) took payments from some of its customers (up to 5%) without reminding them at the time by renewing customers for whom the firm did not have current addresses and so to whom the firm could not send renewals documentation;
 - (5) when the payment cards which customers gave CPP to pay for renewals of Card Protection expired or were cancelled, CPP relied upon an unfair term in its contract with the customer to take payment from another payment card, i.e. one which the customer had registered with CPP for emergency card cancellation purposes. Although customers were sent a renewal pack giving several weeks' advance notice that payment was to be taken, which included the card details that would be used, this was insufficient to fairly obtain the consent of the customer; and
 - (6) in relation to Card Protection customers who cancelled their direct debits, CPP switched to taking payment from one of the cards which the customer had registered with CPP for emergency card cancellation purposes. Although these customers were also sent a renewal pack giving several weeks' advance notice that payment was to be taken, which included the card details that would be used, this was insufficient to obtain the consent of the customer and the payments were taken without the customer's permission.

Breach of Principle 3

- 1.6. From June 2008 at the latest to March 2011, CPP failed to take reasonable care to organise and control its affairs responsibly and effectively because it was aware that significant issues had been raised about the way it sold Card Protection and Identity Protection, and about its compliance and governance arrangements more generally, but failed to take sufficient action to deal with them. In particular, CPP's response to specific compliance deficiencies identified by the FSA and in external Compliance Reports was inadequate.

Aggravating and mitigating factors

- 1.7. The FSA considers CPP's failings to be particularly serious because the problems with CPP's sales continued for more than 6 years, during which time CPP sold and renewed more than 23m policies, and so CPP exposed a very large number of customers to an unacceptable risk of buying products that they did not want or need.
- 1.8. The FSA has taken into account the fact that CPP:
- (1) agreed to amend its Card Protection product and sales process in February 2011 when requested by the FSA and suspended new sales of Identity Protection through its own tele-sales channels when requested by the FSA in March 2011;
 - (2) voluntarily agreed on the request of the FSA in March 2012 to vary its permissions to add a requirement that:
 - (a) it carry out a past business review, overseen by a skilled person appointed under section 166 of FSMA, with a view to paying compensation where appropriate for its own direct sales of Card Protection. CPP estimates that this exercise could cost in the region of c.£8.5m (depending on customer response rates); and
 - (b) it extend the cooling off period from 14 days to 60 days and amend the wording of its renewal packs to give customers a clearer understanding of the benefits and exclusions of their policy;
 - (3) is in the course of implementing recommendations set out in a comprehensive governance review of its business, including:
 - (a) changing its governing structure;
 - (b) making changes to its senior management team;
 - (c) revising its sales call monitoring process by changing the reporting line of its Quality Assurance function which has primary responsibility for monitoring sales calls for compliance so that it reports to the compliance function and not business management; and
 - (d) giving its legal and compliance function an increased role in the sales call compliance monitoring process; and
 - (4) agreed in October 2012 in response to a request by the FSA to apply for a Variation of Permission to impose a requirement by the FSA that:
 - (a) prevents CPP from engaging in future intra-group borrowing arrangements;
 - (b) formalises CPP's existing agreement to cease all new regulated retail sales (apart from where the insurance is sold as part of a package of

products) and not to attempt to retain customers who call to cancel policies; and

- (c) requires CPP to undertake a redress exercise in respect of those customers affected by the failings set out at paragraphs 1.5(5) and 1.5(6) above. CPP estimates that this exercise could cost in the region of c.£6.1m (depending on customer response rates).
- (d) In addition, CPP agreed in October 2012 to an additional requirement under section 166 of FSMA to appoint a skilled person to monitor and report on its claims and complaints handling.

2. DEFINITIONS

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

- (1) “APACS” means the Association for Payment Clearing Services.
- (2) “ARROW” means Advanced Risk Responsive Operating Framework, an assessment FSA supervision make of firms against the FSA’s statutory objectives.
- (3) “Card Protection” means CPP’s Card Protection product.
- (4) “CIFAS” is a fraud prevention service covering the United Kingdom and created in 1988 by a group of retail credit companies and developed in association with the Information Commissioner and the Office of Fair Trading.
- (5) “Compliance Reports” means reports provided by the compliance consulting arms of leading professional services firms in 2007, 2008, 2011 and 2012.
- (6) “CPP” means Card Protection Plan Limited, a regulated entity, the UK subsidiary of CPP Group, and provider of life assistance products and services, including Card Protection and Identity Protection.
- (7) “CPP Group” means CPP Group Plc, a non-regulated entity, listed on the London Stock Exchange.
- (8) “Customer Documentation” means the welcome packs and renewal packs CPP’s customers received after their initial purchase or renewal of Card Protection and Identity Protection.
- (9) “FSA” means the Financial Services Authority.
- (10) “FSMA” means the Financial Services and Markets Act 2000, as amended.
- (11) “Identity Protection” means CPP’s Identity Protection product.
- (12) “Inbound Sales Script” means the script sales agents used when a cardholder called to confirm “safe receipt” of his card or to activate his card.

- (13) “Principle” means one of the Principles for Businesses set out in PRIN 2.1.1 R (Principles for Businesses) of the FSA Handbook.
- (14) “Product Sheets” means the documentation supplementary to the sales scripts which contained additional details about the products.
- (15) “Relevant Period” means 14 January 2005-March 2011.
- (16) “Tele-Sales Materials” means the materials CPP’s sales agents used to make in-bound and out-bound telephone sales of Card Protection or Identity Protection.
- (17) “Tribunal” means the Upper Tribunal (Tax and Chancery Chamber).

3. FACTS AND MATTERS

Background

- 3.1. CPP is an insurance intermediary and a subsidiary of CPP Group. CPP Group is listed on the London Stock Exchange and is a provider of life assistance products and services, operating in 16 countries and with over ten million customers worldwide.
- 3.2. CPP’s two core UK products are Card Protection and Identity Protection. CPP’s offices are in York (sales and head office functions); Tamworth (sales and agents teams); and Chesterfield (sales and agents teams). CPP sold these products to consumers directly through its own sales channels and it also sold them (as explained in more detail below) on an “introduced” basis by selling them to the customers of some of its business partners.
- 3.3. This notice only concerns CPP’s UK sales of Card Protection and Identity Protection.
- 3.4. The principal sales failings which the FSA has identified relate to the period from 14 January 2005 to March 2011. During this period:
 - (1) CPP sold 4.4 million Card Protection and Identity Protection policies and received £188.3 million in customer payments (a proportion of which it paid to its business partners for an introduction fee) for those new sales. CPP renewed 18.7 million Card Protection and Identity Protection policies and received £656.5 million in customer payments (a proportion of which it paid to its business partners for an introduction fee) for those renewals.
 - (2) CPP generated gross profits of £354.5 million and net profits of £79.1 million.
 - (3) CPP paid £46.8 million in dividends to its parent, CPP Group.
- 3.5. CPP employed an automatic renewal approach whereby CPP renewed policies unless a customer contacted CPP to cancel after receiving a renewal pack.

Card Protection – cost and key features

- 3.6. CPP's Card Protection cost approximately £35 per annum (depending on the business partner and when it was sold). The £35 payment is broken down as follows:
- (1) CPP received approximately £34.40 for its "insurance intermediary services" and paid a specified percentage of that to relevant business partners (in some cases up to 60%) for introducing CPP to their customers; and
 - (2) a premium of approximately £0.60 (inclusive of insurance premium tax) which covered the provision of all insurance and non-insurance features of the product.
- 3.7. The policy features varied over time and by business partner, but its key features were:
- (1) "One call stops all," a free telephone number customers could use to call CPP to ask it to inform their card issuers that their cards had been lost or stolen;
 - (2) £5,000 insurance against the cost of any unauthorised use of a customer's card before the customer reports the loss to CPP (or his card issuer);
 - (3) £50,000 to £100,000 (the figure varied during the Relevant Period) insurance against the cost of any unauthorised use of a customer's cards after the customer reports the loss to CPP (or his card issuer);
 - (4) £1,000 insurance for unauthorised calls made on a customer's lost or stolen mobile phone;
 - (5) Emergency loans and delivery of cash to customers who lose their cards while travelling abroad; and
 - (6) "Lost key cover," in which CPP arranges for the replacement of the customer's lost keys.

Identity Protection – cost and key features

- 3.8. CPP's Identity Protection cost approximately £84 per annum (depending on the business partner and when it was sold). The payment is broken down as follows:
- (1) CPP received approximately £68 for its "insurance intermediary services" and paid a specified percentage of that to relevant business partners (in some cases as much as 50%) for introducing CPP to their customers; and
 - (2) a premium of approximately £16 (inclusive of insurance premium tax) which covered the provision of all insurance and non-insurance features of the product.
- 3.9. The policy features varied over time and by business partner, but the key features included:
- (1) access to various monitoring tools and reports which are designed to limit the customer's exposure to identity theft, more specifically:

- (a) access to credit reports and credit monitoring service;
 - (b) the provision for online monitoring of customer's personal information held online;
 - (c) registration with a fraud detection service;
 - (d) credit reports; and
 - (e) CPP helpline;
- (2) caseworker assistance in the event of identity fraud;
 - (3) up to £60,000 of insurance for legal fees and specified out of pocket expenses;
 - (4) payment for lost earnings (up to £500 per week for the first six weeks); and
 - (5) £200 to replace a missing passport and/or driving licence.

The sales channels

- 3.10. CPP sold Card Protection and Identity Protection through several sales channels, including telephone sales, website sales and as a feature within some packaged bank accounts provided by some of their business partners.
- 3.11. The majority of its sales were "introduced sales", sales which occurred when a business partner introduced its customer to CPP to give CPP the opportunity to sell Card Protection and Identity Protection. CPP paid relevant business partners a commission for each original sale and a further commission each time the customer renewed his policy.
- 3.12. Some business partners "introduced" their customers to CPP by affixing a sticker to the new credit or debit cards sent to their customers. The sticker prompted the customer to call a number (which was actually CPP's) either:
 - (1) to activate the card, known as "card activation"; or
 - (2) to confirm that the customer had received the card, known as "safe receipt".
- 3.13. When the customer did call the number CPP also used the conversation to offer Card Protection and/or Identity Protection.
- 3.14. CPP originally purported to make sales on an advised basis. It decided to change to a non-advised basis on 1 July 2008. The basic feature of a non-advised sales process is that a firm should provide information to a customer without recommending the product.

Card Protection sales

Pre-notification cover

- 3.15. As explained above, one feature of Card Protection was “pre-notification cover”. Pre-notification cover provided customers with up to £5,000 of insurance for unauthorised transactions which occurred *before* they notified CPP that their cards were lost or stolen. However, cardholders are not liable for more than the first £50 if the transaction falls within the Consumer Credit Act 1974 (which is very often the case and so this aspect of cover was of very limited value). Further, for transactions that are not covered by that legislation, the customer is only liable for more than the first £50 if they have been “grossly negligent”.

Post-notification cover

- 3.16. Another feature of Card Protection was “post-notification cover”. The post-notification feature purported to provide customers with up to £50,000 or £100,000 of insurance (the figure varied over the Relevant Period) for unauthorised transactions which occurred *after* customers notified CPP that their cards had been lost or stolen. However, cardholders are not liable for unauthorised transactions after they notify their card issuers that their cards have been lost or stolen. Therefore customers did not need this cover and it should not have been used as a marketing feature.

Card Protection sales calls

- 3.17. Sales agents were directed to use the availability of pre- and post-notification cover early on in their sales pitches despite the fact that customers would:
- (1) most likely never need the pre-notification aspect of the product; and
 - (2) never need the post-notification cover.
- 3.18. As a result sales agents failed to give a fair and balanced picture of the utility of Card Protection’s pre- and post-notification cover.
- 3.19. CPP continued to approach its sales pitches in this way despite being alerted to the problem by the FSA on 5 June 2008 (on which see paragraph 3.55 below).

Identity Protection sales

The Tele-Sales Materials

- 3.20. CPP’s sales agents used Tele-Sales Materials to sell Card Protection and Identity Protection policies. The Tele-Sales Materials included the following documents:
- (1) inbound, outbound and service cross-selling sales scripts and inbound alternative sales scripts (which sales agents used when a customer initiated the call to CPP);
 - (2) service cancellation turnaround scripts (which sales agents used to persuade an existing customer who rang to cancel his existing policy not to cancel it);
 - (3) product and facts and figures sheets (which gave sales agents more detailed information about the Card Protection and Identity Protection products and about identity theft than was available in the sales scripts themselves); and

- (4) objection handling sheets (which gave sales agents a list of reasons to use to convince potential customers who originally declined to purchase the product to purchase it).
- 3.21. The Tele-Sales Materials blurred the distinction between advised and non-advised sales, inappropriately emphasised concerns about identity theft and contained misleading facts and figures. An explanation of the problems with the Tele-Sales Materials is set out below, by reference to a specific set of materials (i.e. those in use as at 1 July 2008 immediately after CPP switched to a non-advised sales model).

The inbound sales script

- 3.22. The inbound sales script opened by asking the cardholder to confirm his address, phone number and date of birth because “*Bearing in mind the concerns about identity fraud, I need to confirm that I am speaking to the correct person . . .*”
- 3.23. The script then asked the sales staff to ask the customer a series of questions. It is not clear why this was necessary in the context of a non-advised sale. Moreover, the questions appeared to be designed not to help the sales agent establish the suitability of the product for the customer, but to heighten the customer’s concern about identity theft. The script suggested that ordinary everyday activities like receiving your neighbour’s post and browsing the internet make the cardholder dangerously susceptible to identity theft (“*how do you dispose of your mail? Has your post been intercepted? How would you know? How many times have you received post for your neighbour? How often do you use the internet?*”).

The product sheets

- 3.24. The product sheets were supplementary to the sales scripts and contained details about the products.
- 3.25. The product sheets instructed the sales agent to ask potential customers, “*What do you know about ID theft?*” and then “*What would be your biggest concern if you were to become a victim?*”
- 3.26. The product sheets identified the availability of “*up to £60,000 of insurance to make sure you do not end up out of pocket when clearing your name*” but failed to explain that the insurance only covers administrative and legal expenses. They did not explain that the insurance does not cover debts fraudulently taken out in the individual’s name (although the customer is not liable for such debts in any event).

The objection handling sheets

- 3.27. The objection handling sheets were supplementary to the scripts and instructed sales agents how to handle cardholder’s objections to purchasing the products. The objection handling itself was often inappropriate and in addition the sheets used misleading and unverifiable statistics.
- 3.28. As set out above, CPP had adopted a non-advised sales process. In a non-advised sales process, a firm should simply provide information to the customer without

recommending the product. Despite this, CPP instructed its sales agents to “handle” a potential customer’s objections to buying the product by inappropriately questioning their objections.

3.29. The statistics set out in the objection handling (and in the other Tele-Sales Materials) were often misleading or unsupportable. For example, the objection handling sheets referred to identity theft statistics, but the statistics cited are unverifiable:

(1) In response to a customer’s objection that identity theft will “*never happen to me*” the sales agent was told to respond, “*APACS state 1 out of 5 of us will be a victim of ID crime by the end of the year*”. However:

(a) The UK Payments Administration website, which holds the APACS information, did not contain information to support this statement for identity theft in 2008 and the statistic itself is not supported by any reputable statistics. In fact, in 2008 the UK Payments Administration website published a press release in which APACS criticised CPP for the use of their statistics.

(b) In relation to Identity Protection, CPP’s objection handling sheet instructed sales agents to handle potential customers who are sceptical about the likelihood of identity fraud by saying: “*It can take up to 300hrs to clear your name. Highlight that whilst it’s possible to do this yourself it takes a lot of time; expense and you run the risk of missing important steps.*” APACS’s press releases from 2008 do not support the “*up to 300 hours*” statistic. A CIFAS statistic from 2009 uses “200 hours” as the time it could take in a “total hijack”, but in context it says: “*It can take between 3 and 48 hours of work for typical victims to sort out their lives and clear their names and, in cases where a ‘total hijack’ has occurred involving 20-30 different organisations, it may take a victim over 200 hours before things are back to normal*”.

3.30. Although the Tele-Sales Materials themselves contained inherent flaws, CPP made the situation worse by giving its sales agents scripts which allowed them significant discretion as to what to say in different parts of the sales call.

3.31. These factors combined led to high incidences of mis-selling as evidenced in the actual sales calls themselves which are discussed below.

Identity Protection sales calls

3.32. The FSA identified serious failings in a sample of 99 randomly selected sales calls for Identity Protection and concluded that CPP’s sales agents were engaged in widespread mis-selling.

3.33. In the sales calls themselves, the sales agents failed to give a fair and balanced picture of the risks of identity theft and the need for Identity Protection. More specifically, some sales agents:

- (1) failed to give customers fair and balanced information regarding the risks of identity theft (they relied on misleading and out of date statistics that exaggerated both the extent of identity theft and the time it takes an individual to resolve cases of identity theft). For example, in one call the sales agent referred to a “40% increase in identity theft in the last year alone”, but CIFAS’ website indicated a 1% increase in identity theft cases between 2009 and 2010.
- (2) told customers that they were legally liable to repay debts fraudulently taken out in their names when this was not true.
- (3) misled customers about the items they were already covered for under relevant consumer protection legislation.
- (4) failed to make customers aware of key exclusions or key conditions in the Identity Protection policy.
- (5) provided customers with claims data exaggerating the scope of Identity Protection cover and the benefits of Identity Protection, including the extent of CPP caseworker assistance and coverage of online monitoring. For example, a sales agent told one customer that the £60,000 insurance covered “*basically, anything you’re out of the pocket for, we would pay*”. In addition, he told the potential customer that criminals were “*leaving people liable with the bills, debts and the problems of sorting it all out*”. While the sales agent made some reference to legal and administrative costs, he left the potential customer with the impression that the £60,000 insurance would cover any debts a person fraudulently using a person’s identity incurred. The £60,000 does not cover any debts fraudulently incurred in the customer’s name (which the customer would not be liable for in any event). It only covers the legal and administrative costs required to deal with the problem.
- (6) used inappropriate objection handling so that when customers raised objections to buying Identity Protection, sales agents handled those objections by questioning why the customer objected (by using sales techniques described above in (1) – (5)), or by emphasising the customer’s ability to cancel the product after buying it. The effect of this objection handling was to persuade customers to change their minds and resulted in undue pressure on customers to buy the product.
- (7) sold the product to customers who could not make full use of prominent product features, for example they failed to explain to customers who did not have internet access that they would not be able to use on-line monitoring.

Welcome packs

- 3.34. Once a customer agreed to purchase Card Protection or Identity Protection he would receive a “welcome pack” in the post. CPP offered one year term or three year term policies.
- 3.35. The welcome packs for Card Protection sales repeated the failings identified in the Tele-sales materials as detailed above at paragraphs 3.15 to 3.19. In particular, the

welcome packs prominently featured pre-notification cover without adequate clarification of when such cover would be needed by the customer. The welcome packs also prominently featured post-notification cover which would never be needed by customers.

- 3.36. The welcome packs for Identity Protection sales identified the provision of “*up to £60,000 for restoring your identity*” but failed to explain clearly that this insurance only covered administrative and legal expenses. The welcome packs did not explain that the insurance did not cover debts fraudulently taken out in the individual’s name (although the individual was not liable for such debts in any event).

The renewals process

- 3.37. Approximately three to six weeks before the policy automatically renewed, CPP would send a renewal pack to the customer. The renewal pack did not clearly set out what the customer should do in order to cancel. Rather, the renewal pack was drafted on the basis that the policy would simply renew (for example, “*Great news! Your Identity Protection insurance is renewing*”). The renewal packs also repeated many of the exaggerated claims and inaccurate statistics sales agents used to sell the products in the first place.
- 3.38. In some instances, as explained further below, customers never received the letter because CPP failed to keep an up-to-date customer address list. In those cases, the customer was unlikely to become aware that CPP had renewed his policy unless he reviewed the credit or debit card statement that captured that payment.
- 3.39. By that time, it was generally too late to cancel the policy because, as provided in the policy terms and conditions:
- (1) the policy automatically renewed within 14 days from the date of the notification letter; and
 - (2) once the cancellation window closed, a customer was required to pay for the whole year and it was not possible to receive even a partial refund.
- 3.40. Flaws in the design of CPP’s policy administration process meant that it charged some customers for the products in reliance on an unfair term in the terms and conditions and/or without ensuring that the customer authorised payment. This happened to Card Protection customers through “Autopaycard” and to customers of both Card Protection and Identity Protection because of the way CPP dealt with customers for whom the firm knew it did not have up to date addresses.

Autopaycard

- 3.41. CPP took payments from some Card Protection customers by an “Autopaycard” feature, using a term in the policy’s terms and conditions which said that CPP could take payment from another card registered with CPP in the event that payment could not be taken from the card originally specified for payment.

- 3.42. The FSA considers that the term was unfair because CPP used information provided to it by customers in order to benefit from a Card Protection feature that was ostensibly designed to protect the customer (“one-call stops all”) and used it for its own benefit by taking a payment from any card the customer registered for this feature. Whilst customers were sent a renewal pack giving several weeks’ advance notice that payment was to be taken, which included the card details that were to be used, the FSA does not consider that this was sufficient to obtain the consent of the customer to taking payment from that alternative card.
- 3.43. CPP used the following process:
- (1) CPP promoted the “one-call stops all” feature as a valuable feature of Card Protection. It allowed a Card Protection customer to register not just the credit or debit card that prompted him to call CPP in the first place, but to register all of his credit and debit cards with CPP.
 - (2) Then, if the customer’s wallet was lost or stolen, he would telephone CPP and CPP would telephone all the card issuers of all cards the customer registered with CPP, “one call stops all”.
 - (3) This was the ostensible purpose of the “one call stops all” feature.
- 3.44. However, the terms and conditions also stated that CPP could take renewal payments not just from the card from which the customer originally specified that payments should be taken, but from any card that the customer registered with CPP for “one call stops all” protection. Notwithstanding the fact that CPP sent the customer a notification before taking payment from an alternative card, we consider this practice to have the potential to result in an unfair outcome for the customer. We also consider the contract terms stating the practice to be unfair under the Unfair Terms in Consumer Contracts Regulations 1999.
- 3.45. The FSA accepts that the mere fact that a card expires or is cancelled does not necessarily mean that the customer did not intend to cancel the policy. Nevertheless, the use of the Autopaycard term gave rise to a risk that, even if a customer intended for his Card Protection policy to cease when he cancelled the original card he used to pay, or it expired, it did not. CPP instead continued to take payments, but took them from another of the cards the customer registered with CPP for “one call stops all” protection without taking adequate steps to obtain the customer’s consent to taking payments from that card.

CPP took payments from customers without permission

- 3.46. CPP also took payments from alternative cards registered for emergency card cancellation purposes when a customer cancelled a direct debit without seeking the customer’s consent. Although such customers were sent a renewal pack giving several weeks’ advance notice, which included details of the card from which payment was due to be taken, there was no contractual term permitting payment to be taken in this way.

Gone-aways

3.47. CPP continued to take payments from Card Protection and Identity Protection customers whose addresses were no longer current. This amounted to about 5% of CPP's customer population. CPP used the following process:

- (1) CPP would send renewal packs to customers.
- (2) Sometimes the Royal Mail or the property's current occupant would return the renewal pack to CPP explaining that the addressee no longer lived at that address.
- (3) CPP would cease sending the renewal pack to the customer, but would continue to automatically renew the customer's policy and continue to take the payment.
- (4) CPP categorised such customers as "Gone-aways" and continued to generate revenue from them, without any way of confirming whether the customer realised that he had the benefit of the policy or not.
- (5) CPP did include details of the product and a telephone number that customers could use to update CPP with a new address on the narrative entry included on the bank card or credit card statement showing the payment being taken. CPP should, however, have put in place a system to deal with these customers that ensured that it did not continue to renew policies for customers who it could not confirm were aware that CPP:
 - (a) was continuing to take payments from them; or
 - (b) was continuing to renew a policy the customer might no longer want.

Cancellation turn-arounds

3.48. CPP gave its sales agents cancellation turn-around targets and incentives. This created a risk of sales agents using inappropriate objection handling techniques to discourage customers who tried to cancel their policies.

FSA and Compliance Reports identified serious concerns throughout the Relevant Period

3.49. CPP was aware of significant concerns with its sales and its Tele-Sales Materials and Customer Documentation, and with its compliance and governance arrangements more generally, on the basis of:

- (1) FSA Arrow visits and follow up correspondence; and
- (2) Compliance Reports prepared by third party consultants.

The 2005 ARROW – CPP's first ARROW visit

3.50. FSA supervisors undertook their first ARROW visit to CPP in April 2005. During this period, CPP made sales on an advised basis.

- 3.51. The FSA categorised CPP's effect on the FSA's statutory objectives as "medium high". It summarised its findings in a letter and risk mitigation programme identifying actions CPP needed to take to mitigate the risks the FSA identified.
- 3.52. The FSA made the following observations and recommendations:
- (1) CPP's governance arrangements were not well established and they were inconsistent with the nature, size and complexity of the business.
 - (2) The individuals on the Group board who might be able to exert significant influence over the regulated firm should hold the appropriate controlled functions.
 - (3) CPP did not have an established risk management process and there was "*little serviceable data on compliance issues and risks*" affecting the firm.
 - (4) The risk management processes, policies and procedures within the firm need to be established and embedded.
 - (5) The "*lack of a well defined and robust risk management process could lead to the firm failing to identify and mitigate key risks to the business and consumers, which could lead to failure of the firm*".

The 2007 Compliance Report

- 3.53. CPP took a number of steps in response to the FSA's 2005 ARROW visit and findings including commissioning the compliance consulting arm of a leading professional services firm to undertake a high level compliance review for it to prepare for its next FSA ARROW visit. The consultant's overall impression when it reported in 2007 was that "*CPP has many component parts in place to evidence appropriate governance, although some areas need to be further formalised and enhanced*".
- 3.54. One of the key areas in the consultant's recommendations was around the governance structures of CPP's Board and UK leadership team, and how the governance arrangements were documented.

The 2008 ARROW – CPP's second ARROW visit

- 3.55. The FSA conducted its second ARROW visit from 11-13 February 2008 and set out its findings (after a series of additional meetings) in a letter dated 5 June 2008. At this point, CPP still made advised sales. This would change in July 2008.
- 3.56. Supervision reflected its renewed concerns about CPP by increasing the firm's risk rating to "high" and by requiring CPP to commission a report on its sales process and controls framework under section 166 of FSMA.
- 3.57. The FSA explained:

"Our overall view is that the risk to our statutory objectives has increased markedly to a high rating and we recognise the Regulated Group as a significant outlier to its peers."

- 3.58. The FSA found that the advice given to customers during the sales process did not comply with several ICOBS requirements and Principles. In particular, the FSA found that *“the description of the products in the sales discussion and in written materials is potentially misleading about the cover provided (in particular the significance of the insurance element [i.e. the unauthorised transaction cover] of the Card Protection product given the protection already provided by lenders under the Banking Code)”*.
- 3.59. The FSA also provided the following as examples of the non-compliant advice it had found:
- (1) sales agents failed to make a personal recommendation;
 - (2) sales agents failed to assess customers’ demands and needs; and
 - (3) the approach to supplying regulatory information was to require the customer to positively ask for it, rather than to agree not to receive it.
- 3.60. The FSA also made the following findings and observations:
- (1) Sales controls – the FSA was “disappointed” by the quality of sales calls and wanted “comfort” that CPP was “capable of” identifying the same issues the FSA identified.
 - (2) Corporate governance – the FSA was concerned about elements of CPP’s UK leadership team, a group of senior CPP business leaders, and their lack of acceptance of many of the recommendations in the 2007 Compliance Report.
 - (a) CPP provided conflicting information about decision making in the firm. It was unclear which body took decisions, CPP’s board or the UK leadership team. The concern was heightened because the UK leadership team was not a formal body and the matters discussed and decisions taken were not recorded.
 - (b) The FSA said that it was “very disappointed” that CPP failed to accept many of the recommendations set out in the 2007 Compliance Report.
 - (3) Compliance oversight – the FSA was particularly concerned because CPP had failed to identify these issues itself. The FSA was also concerned that the firm’s practices did not match its documentation and that its compliance function failed to identify ICOBS breaches.
 - (4) Treating Customers Fairly – Complaints – the FSA noted that it found letters offering goodwill payments to customers, but it was concerned that CPP was failing to learn lessons from the complaints.

The 2008 Compliance Report

- 3.61. As set out in the ARROW reports, the FSA was dissatisfied with CPP’s failure to develop a systematic approach to its tele-sales, the mechanisms it had in place to review the tele-sales for compliance and its approach to compliance generally. Because CPP had not been able to resolve the problems itself, the FSA required the

firm to commission a report under section 166 of FSMA from the compliance consulting arm of a leading professional services firm.

- 3.62. The consultant presented its report to CPP in October 2008. The consultant examined the firm's non-advised sales processes in its 2008 Report and identified instances when the telephone sales processes were not applied in practice, resulting in actual or potential breaches of the FSA's requirements. For example, the consultant found in its review of 109 sales that in 59 sales (54%) the customer's explicit consent to receiving limited status and product disclosure was not obtained, and in 54 sales (49%) the key exclusions and limitations were not explained in sufficient detail or sufficiently clearly.
- 3.63. The 2008 Compliance Report warned CPP that sales agents were continuing to provide advice even though CPP had moved to selling on a non-advised basis. It noted that the call monitoring regime that was in place at the time was not sufficiently robust and failed to identify and remedy a number of instances where advice was provided.
- 3.64. The consultant tested CPP's sales processes and supporting systems and controls shortly after they were implemented and noted in its report that in its experience "*any new or revised systems, controls, policies or procedures need time to implement and embed*". The consultant also noted that, at the time, CPP's senior management team appeared to maintain strict oversight over the new sales processes. However, the consultant also noted that, as the call monitoring regime had failed to identify and remedy a number of instances whereby advice was provided, it could be argued that "*the transition from an advised to a non-advised sales process was not sufficiently controlled*".

The 2011 Compliance Report

- 3.65. CPP's compliance function was required to keep CPP aware of regulatory changes, and to prepare materials to teach sales agents how to sell compliantly, participate and direct those training sessions, and vet Sales Materials for compliance. The compliance function convinced CPP to commission a report from the compliance consulting arm of another leading professional services firm in 2010. The consultant issued its report in January 2011 and made the following observations and recommendations:
 - (1) "*The Compliance and legal functions are already significantly resource constrained and require additional resource to recover current planned activities and address identified gaps and areas for improvement*".
 - (2) "*The allocation of all legal and regulatory responsibilities should be clarified and documented*".
 - (3) "*We are not clear on the extent to which the regulatory dimension is incorporated into business planning*".

- (4) *“A number of potential internal conflicts arise from the Compliance function’s range of activities covering design, production, approval and subsequent compliance monitoring of procedures, scripts and documentation”.*
- (5) *“Management indicated that the compliance monitoring programme is currently under strain, is being juggled with competing regulatory responsibilities, and is behind plan in a number of areas”*

3.66. CPP increased its compliance resource in response to this report and, after FSA intervention, CPP agreed to amend its Card Protection product and sales process in February 2011 and stopped new sales of Identity Protection through its own tele-sales channels in March 2011.

The 2012 Compliance Report

3.67. The Group commissioned a further report from the compliance consulting arm of a third leading professional services firm in 2011-2012. The report, completed in 2012, was issued after the FSA had intervened and put a stop to CPP’s main sales failings as described above. The report identified significant high level issues showing that CPP still had a significant compliance problem. The Executive Summary of the report included a conclusion that *“the current three lines of defence model (the best practice model for good corporate governance) used within the UK operation, is currently not functioning effectively as it has not been fully adopted and the clarity of responsibilities for regulatory support is not understood.”*

Analysis of CPP’s response to the Compliance Reports

3.68. CPP took a large number of steps to improve its systems and controls during the Relevant Period, including in response to specific issues raised in response to the Compliance Reports detailed above. Among other steps, CPP introduced the following during the Relevant Period:

- (1) a remuneration policy where compliance was taken into account in the remuneration of sales agents and other staff;
- (2) the creation and regular review of risk maps and more detailed risk registers;
- (3) *“treating customers fairly”* (TCF) governance arrangements, including a TCF *“dashboard”* capturing key customer and compliance management information;
- (4) various changes in personnel in compliance and other key roles; and
- (5) the setting up of internal fora for compliance issues to receive regular attention and debate.

3.69. However, overall CPP’s approach to compliance fell short of the standards the FSA expects, especially in light of the wide range of issues raised in the Compliance Reports. While CPP did try to respond to specific issues raised in the Compliance Reports (and in some cases it was successful in doing so, for example in improving its management information), CPP failed to deal with the fact that it had a serious compliance problem overall. In particular, it failed to put in place the necessary

safeguards to avoid the widespread mis-selling which occurred for over six years. CPP also continued to emphasise insurance cover which customers did not in fact need (i.e. the Card Protection post-notification unauthorised transaction cover) or which was significantly limited (i.e. the Card Protection pre-notification unauthorised transaction cover) despite a clear warning from the FSA that CPP was potentially misleading customers given the existing protection already provided to customers by lenders.

4. FAILINGS

4.1. From January 2005 until March 2011 CPP was in breach of:

- (1) Principle 7 because it failed to pay due regard to its customers' information needs and failed to communicate information to them in a way which was clear, fair and not misleading because:
 - (a) CPP sold its Card Protection product by emphasising to customers that they would benefit from up to £50,000 or £100,000 (the figure varied over the relevant period) worth of post-notification insurance cover when in fact customers did not need this cover;
 - (b) in relation to the pre-notification aspects of the Card Protection insurance cover, it failed to explain the very limited circumstances in which customers would need the cover; and
 - (c) in relation to its Identity Protection product it overstated the risks and repercussions of identity theft in its sales and Customer Documentation.
- (2) Principle 6 because it failed to pay due regard to the interests of its customers by designing a sales process which promoted an excessive focus on sales, revenue and commercial objectives at the expense of treating customers fairly in that it:
 - (a) inappropriately encouraged sales agents to be overly persistent in persuading potential customers of both products to purchase them even after the customers had made it clear that they did not wish to buy them;
 - (b) gave its sales agents targets for successfully dissuading customers who contacted CPP to cancel their policies;
 - (c) did not contain sufficient safeguards to prevent sales agents inappropriately seeking to persuade customers to buy the products on the basis that customers could cancel them during the cooling-off period;
 - (d) took payments from some of its customers (up to 5%) without reminding them at the time by renewing customers for whom the firm did not have current addresses and so to whom the firm could not send renewals documentation;

- (e) when the payment cards which customers gave CPP to pay for renewals of Card Protection expired or were cancelled, CPP relied upon an unfair term in its contract with the customer to take payment from another payment card, i.e. one which the customer had registered with CPP for emergency card cancellation purposes; and
- (f) in relation to customers who cancelled their direct debits, CPP switched to taking payment from an alternative card without permission.

4.2. CPP breached Principle 3 between June 2008 and March 2011 by failing to take reasonable care to organise and control its affairs responsibly and effectively because it was aware that significant issues had been raised about the way it sold Card Protection and Identity Protection, and about its compliance and governance arrangements more generally, but failed to take sufficient action to deal with them. In particular, CPP's response to specific compliance deficiencies identified by the FSA and in external Compliance Reports was inadequate. One example of this is that CPP should have made sure it was aware of the existing protection already provided to customers by the Banking Code and:

- (1) entirely removed the post-notification cover from all marketing of the Card Protection product; and
- (2) properly explained to customers the extremely limited value of the pre-notification cover

especially given the FSA's clear warning in June 2008 that CPP was potentially misleading customers given the existing protection already provided to customers by lenders.

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

5. SANCTION

5.1. In light of the FSA's findings, the FSA considers that the imposition of a public sanction is both justified and proportionate in all the circumstances.

5.2. In determining the financial penalty, the FSA has had regard to its policy on the imposition of financial penalties which is set out in Chapter 6 of the Decision Procedure & Penalties Manual (DEPP) and forms part of the FSA Handbook. The FSA has also had regard to Chapter 7 of its Enforcement Guide.

5.3. On 6 March 2010, the FSA's new penalty framework came into force. CPP's misconduct covers a period straddling before and after 6 March 2010 but the FSA considers that the gravamen of the misconduct is before 6 March 2010. The FSA has therefore assessed the financial penalty under the regime in force prior to 6 March 2010.

5.4. DEPP 6.5.2G sets out the factors that may be of particular relevance in determining the appropriate level of financial penalty for a firm or approved person. The criteria are not exhaustive and all relevant circumstances of the case are taken into

consideration. In determining the appropriate level of sanction, the FSA has had regard to the factors from DEPP 6.5.2G listed below.

Deterrence

- 5.5. The financial penalty is required to promote high standards of regulatory conduct by deterring firms which have breached regulatory requirements from committing further breaches, deterring other firms from committing similar breaches and demonstrating generally to firms the benefits of compliant behaviour.

The nature, seriousness and impact of the breach in question / The extent to which the breach was deliberate or reckless / Conduct following the breach

- 5.6. The FSA has had regard to the seriousness of the breaches, including the nature of the requirements breached, the nature and duration of the breaches and the number of customers who were impacted.
- 5.7. For the reasons set out above, the FSA considers the breaches to be particularly serious in this case. The breaches occurred for more than six years and more than 23m policies were sold and renewed by CPP during the Relevant Period.
- 5.8. The FSA has taken into account the aggravating and mitigating factors outlined at paragraphs 1.7 and 1.8 above.

The size, financial resources and other circumstances of the firm

- 5.9. The FSA has considered the financial position of CPP. Based on the evidence made available to the FSA, it considers that CPP is able to pay the penalty. However, as a result of CPP's current financial position, the FSA has agreed to allow CPP to pay instalments as set out in paragraph 6.2 below.

Disciplinary record and compliance history

- 5.10. CPP has not previously been the subject of disciplinary action by the FSA.

Previous action taken by the FSA in relation to similar findings

- 5.11. In determining whether and what financial penalty to impose on CPP, the FSA has taken into account action taken by the FSA in relation to other authorised persons for comparable behaviour.

Conclusion as to financial penalty

- 5.12. Accordingly, the FSA considers it necessary and proportionate to impose a financial penalty of £10.5 million, pursuant to section 206 of the Act, on the grounds that CPP failed to take reasonable care to organise and control its affairs responsibly and effectively, failed to treat customers fairly, and failed to communicate with customers in a way that was clear, fair and not misleading.

6. PROCEDURAL MATTERS

Decision maker

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

Important

- 6.2. This Final Notice is given under, and in accordance with section 390 of FSMA.

Manner of and time for payment

- 6.3. The financial penalty is to be paid in 6 instalments. The first instalment of £2 million must be paid by CPP to the FSA within 14 days of the date of the Final Notice. The next instalment of £2 million must be paid by 1 June 2013. The final four instalments, each of £1.625 million, must then be paid by 1 March 2014, 1 June 2014, 1 September 2014 and 1 December 2014 respectively.

If the financial penalty is not paid

- 6.4. If any instalment is not paid by the due date for that instalment then the financial penalty becomes payable immediately and in full. The FSA may recover the outstanding amount as a debt owed by CPP and due to the FSA.

Publicity

- 6.5. Sections 391(4), 391(6) and 391(7) of FSMA apply to the publication of information about the matter to which this Notice relates. Under those provisions, the FSA must publish such information about the matter to which this Notice relates as the FSA considers appropriate. The information may be published in such manner as the FSA considers appropriate. However, the FSA may not publish information if such publication would, in the opinion of the FSA, be unfair to you or prejudicial to the interests of consumers.
- 6.6. The FSA intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

FSA contacts

- 6.7. For more information concerning this matter generally, contact Greg Sachrajda (direct line: 020 7066 3746) or Maria Gouvas (direct line: 020 7066 3552) at the FSA.

Georgina Philippou

Head of Department

FSA Enforcement and Financial Crime Division

ANNEX A

Relevant Statutory Provisions, Rules and Guidance

7. STATUTORY PROVISIONS

- 7.1. The FSA's statutory objectives include the protection of customers. See s 2(5) FSMA.
- 7.2. Section 206 of FSMA 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”.

- 7.3. CPP is an authorised person for the purposes of section 206 of FSMA. The requirements imposed on authorised persons include those set out in the FSA's rules made under section 138 of FSMA.

8. REGULATORY PROVISIONS

- 8.1. In exercising its power to issue a financial penalty, the FSA must have regard to the relevant provisions in the FSA Handbook of rules and guidance (“FSA Handbook”).
- 8.2. In deciding on the above action, the FSA has also regard to guidance published in the FSA Handbook and set out in the Regulatory Guides, in particular the Decision Procedure and Penalties Manual (“DEPP”).

Principles for Businesses

- 8.3. The FSA's Principles for Businesses (“PRIN”) are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the FSA's Handbook. They derive their authority from the FSA's rule-making powers as set out in FSMA and reflect the FSA's regulatory objectives. The relevant Principles are as follows:
- (1) Principle 3 (Management and control): *“A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”.*
 - (2) Principle 6 (Customers' interests): *“A firm must pay due regard to the interests of its customers and treat them fairly”.*
 - (3) Principle 7 (Communications with clients): *“A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading”.*

Decision Procedure and Penalties Manual

- 8.4. Guidance on the imposition and amount of penalties is set out in Chapter 6 of DEPP. Changes to DEPP were introduced on 6 March 2010. Given that the majority of the

misconduct occurred prior to that date, the FSA has had regard to the provisions of DEPP in force prior to that date.

- 8.5. DEPP 6.1.2 provides that the principal purpose of imposing a financial penalty is to “*promote high standards of regulatory and/or market conduct by deterring persons who have committed breaches from committing further breaches, helping to deter other persons from committing similar breaches, and demonstrating generally the benefits of compliant behaviour*”.
- 8.6. DEPP 6.5.2 sets out some of the factors that may be taken into account when the FSA determines the level of a financial penalty that is appropriate and proportionate to the misconduct as follows:
- (1) deterrence;
 - (2) the nature, seriousness and impact of the breach in question;
 - (3) the extent to which the breach was deliberate and reckless;
 - (4) whether the person on whom the penalty is to be imposed is an individual;
 - (5) the size, financial resources and other circumstances of the person on whom the penalty is to be imposed;
 - (6) the amount of benefit gained or loss avoided;
 - (7) the difficulty of detecting the breach;
 - (8) conduct following the breach;
 - (9) disciplinary record and compliance history;
 - (10) other action taken by the FSA;
 - (11) action taken by other domestic or international regulatory authorities;
 - (12) FSA guidance or other published materials; and
 - (13) the timing of any agreement as to the amount of the penalty.

Enforcement Manual

- 8.7. The FSA has also had regard to the provisions of the Enforcement Manual (“ENF”) in force prior to 28 August 2007, in relation to misconduct which occurred prior to that date.