

**ADVANCED GCE
MATHEMATICS (MEI)**

4754A

Applications of Advanced Mathematics (C4) Paper A

QUESTION PAPER

Candidates answer on the printed answer book.

OCR supplied materials:

- Printed answer book 4754A
- MEI Examination Formulae and Tables (MF2)

Other materials required:

- Scientific or graphical calculator

**Monday 13 June 2011
Morning**

Duration: 1 hour 30 minutes

INSTRUCTIONS TO CANDIDATES

These instructions are the same on the printed answer book and the question paper.

- The question paper will be found in the centre of the printed answer book.
- Write your name, centre number and candidate number in the spaces provided on the printed answer book. Please write clearly and in capital letters.
- **Write your answer to each question in the space provided in the printed answer book.** Additional paper may be used if necessary but you must clearly show your candidate number, centre number and question number(s).
- Use black ink. Pencil may be used for graphs and diagrams only.
- Read each question carefully. Make sure you know what you have to do before starting your answer.
- Answer **all** the questions.
- Do **not** write in the bar codes.
- You are permitted to use a scientific or graphical calculator in this paper.
- Final answers should be given to a degree of accuracy appropriate to the context.

INFORMATION FOR CANDIDATES

This information is the same on the printed answer book and the question paper.

- The number of marks is given in brackets [] at the end of each question or part question on the question paper.
- You are advised that an answer may receive **no marks** unless you show sufficient detail of the working to indicate that a correct method is being used.
- The total number of marks for this paper is **72**.
- The printed answer book consists of **16** pages. The question paper consists of **4** pages. Any blank pages are indicated.
- This paper will be followed by **Paper B: Comprehension**.

INSTRUCTION TO EXAMS OFFICER / INVIGILATOR

- Do not send this question paper for marking; it should be retained in the centre or destroyed.

Section A (36 marks)

1 Express $\frac{1}{(2x+1)(x^2+1)}$ in partial fractions. [5]

2 Find the first three terms in the binomial expansion of $\sqrt[3]{1+3x}$ in ascending powers of x . State the set of values of x for which the expansion is valid. [5]

3 Express $2 \sin \theta - 3 \cos \theta$ in the form $R \sin(\theta - \alpha)$, where R and α are constants to be determined, and $0 < \alpha < \frac{1}{2}\pi$.

Hence write down the greatest and least possible values of $1 + 2 \sin \theta - 3 \cos \theta$. [6]

4 A curve has parametric equations

$$x = 2 \sin \theta, \quad y = \cos 2\theta.$$

(i) Find the exact coordinates and the gradient of the curve at the point with parameter $\theta = \frac{1}{3}\pi$. [5]

(ii) Find y in terms of x . [2]

5 Solve the equation $\operatorname{cosec}^2 \theta = 1 + 2 \cot \theta$, for $-180^\circ \leq \theta \leq 180^\circ$. [6]

6 Fig. 6 shows the region enclosed by part of the curve $y = 2x^2$, the straight line $x + y = 3$, and the y -axis. The curve and the straight line meet at P (1, 2).

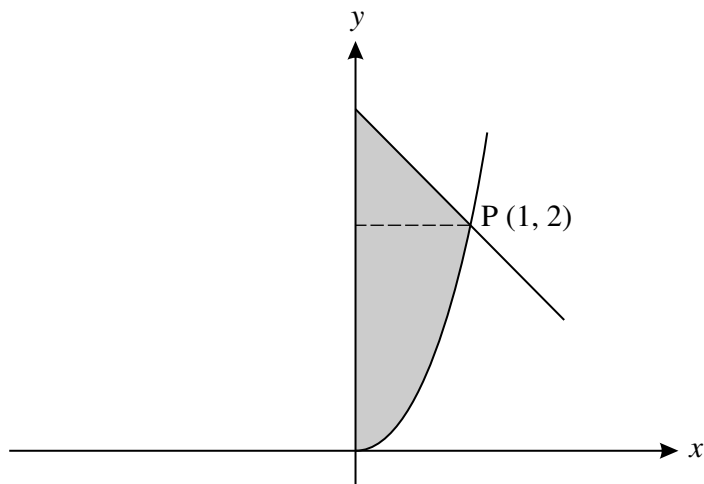


Fig. 6

The shaded region is rotated through 360° about the y -axis. Find, in terms of π , the volume of the solid of revolution formed. [7]

[You may use the formula $V = \frac{1}{3}\pi r^2 h$ for the volume of a cone.]

Section B (36 marks)

- 7 A piece of cloth ABDC is attached to the tops of vertical poles AE, BF, DG and CH, where E, F, G and H are at ground level (see Fig. 7). Coordinates are as shown, with lengths in metres. The length of pole DG is k metres.

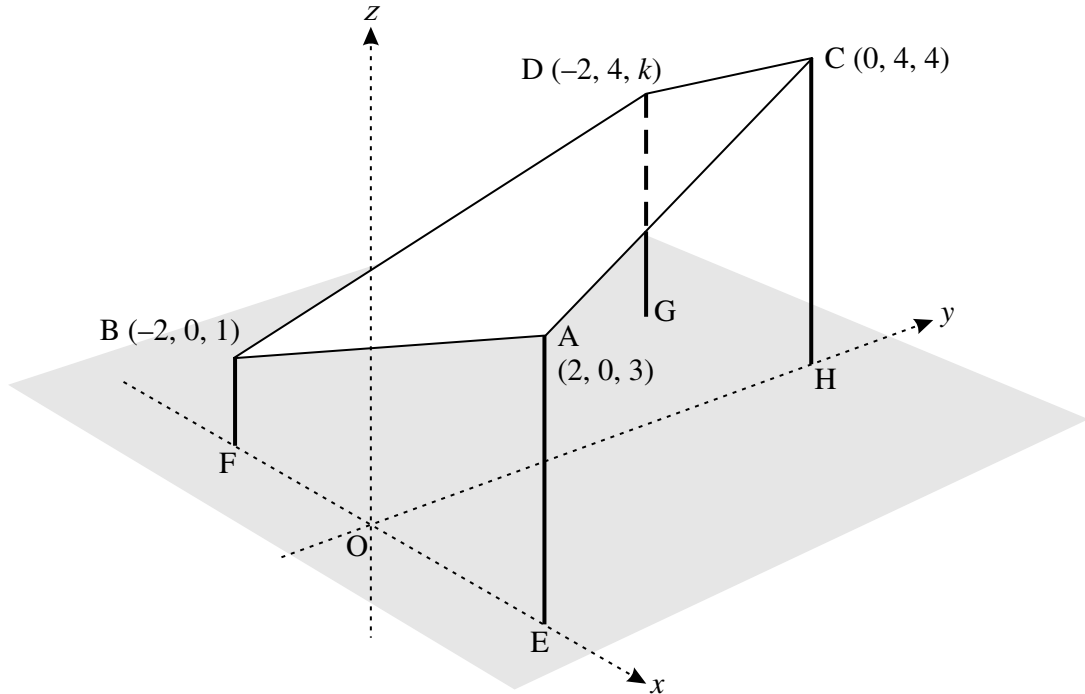


Fig. 7

- (i) Write down the vectors \vec{AB} and \vec{AC} . Hence calculate the angle BAC. [6]
- (ii) Verify that the equation of the plane ABC is $x + y - 2z + d = 0$, where d is a constant to be determined.
Calculate the acute angle the plane makes with the horizontal plane. [7]
- (iii) Given that A, B, D and C are coplanar, show that $k = 3$.
Hence show that ABDC is a trapezium, and find the ratio of CD to AB. [5]

[Question 8 is printed overleaf.]

- 8 Water is leaking from a container. After t seconds, the depth of water in the container is x cm, and the volume of water is V cm³, where $V = \frac{1}{3}x^3$. The rate at which water is lost is proportional to x , so that $\frac{dV}{dt} = -kx$, where k is a constant.

(i) Show that $x \frac{dx}{dt} = -k$. [3]

Initially, the depth of water in the container is 10 cm.

(ii) Show by integration that $x = \sqrt{100 - 2kt}$. [4]

(iii) Given that the container empties after 50 seconds, find k . [2]

Once the container is empty, water is poured into it at a constant rate of 1 cm³ per second. The container continues to lose water as before.

(iv) Show that, t seconds after starting to pour the water in, $\frac{dx}{dt} = \frac{1-x}{x^2}$. [2]

(v) Show that $\frac{1}{1-x} - x - 1 = \frac{x^2}{1-x}$.

Hence solve the differential equation in part (iv) to show that

$$t = \ln\left(\frac{1}{1-x}\right) - \frac{1}{2}x^2 - x. \quad [6]$$

(vi) Show that the depth cannot reach 1 cm. [1]

Copyright Information

OCR is committed to seeking permission to reproduce all third-party content that it uses in its assessment materials. OCR has attempted to identify and contact all copyright holders whose work is used in this paper. To avoid the issue of disclosure of answer-related information to candidates, all copyright acknowledgements are reproduced in the OCR Copyright Acknowledgements Booklet. This is produced for each series of examinations and is freely available to download from our public website (www.ocr.org.uk) after the live examination series. If OCR has unwittingly failed to correctly acknowledge or clear any third-party content in this assessment material, OCR will be happy to correct its mistake at the earliest possible opportunity. For queries or further information please contact the Copyright Team, First Floor, 9 Hills Road, Cambridge CB2 1GE.

OCR is part of the Cambridge Assessment Group; Cambridge Assessment is the brand name of University of Cambridge Local Examinations Syndicate (UCLES), which is itself a department of the University of Cambridge.

**ADVANCED GCE
MATHEMATICS (MEI)**

4754B

Applications of Advanced Mathematics (C4) Paper B: Comprehension

Candidates answer on the question paper.

OCR supplied materials:

- Insert (inserted)
- MEI Examination Formulae and Tables (MF2)

Other materials required:

- Scientific or graphical calculator
- Rough paper

**Monday 13 June 2011
Morning**

Duration: Up to 1 hour



Candidate forename		Candidate surname	
-----------------------	--	----------------------	--

Centre number						Candidate number				
---------------	--	--	--	--	--	------------------	--	--	--	--

INSTRUCTIONS TO CANDIDATES

- The insert will be found in the centre of this document.
- Write your name, centre number and candidate number in the boxes above. Please write clearly and in capital letters.
- Write your answer to each question in the space provided. Additional paper may be used if necessary but you must clearly show your candidate number, centre number and question number(s).
- Use black ink. Pencil may be used for graphs and diagrams only.
- Read each question carefully. Make sure you know what you have to do before starting your answer.
- Answer **all** the questions.
- Do **not** write in the bar codes.
- The insert contains the text for use with the questions.
- You are permitted to use a scientific or graphical calculator in this paper.
- Final answers should be given to a degree of accuracy appropriate to the context.

INFORMATION FOR CANDIDATES

- The number of marks is given in brackets [] at the end of each question or part question.
- You may find it helpful to make notes and do some calculations as you read the passage.
- You are **not** required to hand in these notes with your question paper.
- You are advised that an answer may receive **no marks** unless you show sufficient detail of the working to indicate that a correct method is being used.
- The total number of marks for this paper is **18**.
- This document consists of **4** pages. Any blank pages are indicated.

- 1** In lines 59 and 60, the text says “In that case the proportion suffering such an attack would be 6.4%.”

Explain how this figure was obtained.

[1]

1	

- 2** (i) In lines 8 to 10, the article says “Some banks do not allow numbers that begin with zero, numbers in which the digits are all the same (such as 5555) or numbers in which the digits are consecutive (such as 2345 or 8765).”

How many different 4-digit PINs can be made when all these rules are applied?

[3]

- (ii) At the time of writing, the world population is 6.7×10^9 people. Assuming that, on average, each person has one card with a 4-digit PIN (subject to the rules in part (i) of this question), estimate the average number of people holding cards with any given PIN. Give your answer to an appropriate degree of accuracy.

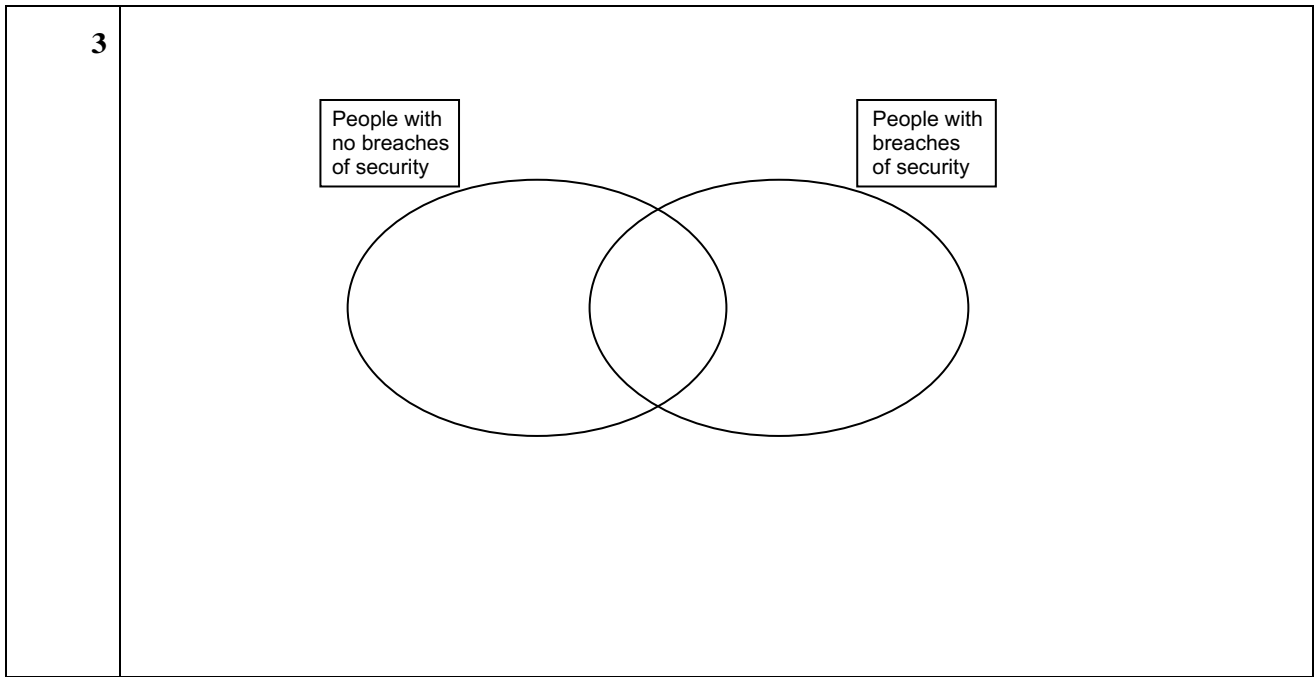
[2]

2 (i)	
2 (ii)	

- 3 In lines 46 and 47, the text says “Of the 11 people with unauthorised transactions, 3 could explain them as breaches of card security (typically losing the card) but 9 could not”

Place numbers in the three regions of the diagram consistent with the information in this sentence.

[2]



- 4 In lines 101 and 102, the text says “The total number of transactions for those who responded has been estimated as 100 000 for the 3½ years covered by the survey.”

Estimate the number of transactions per person per day that would give this figure.

[2]

4	

- 5 The survey described in the article was based on a small sample.

State one conclusion which is unlikely to be influenced by the size of the sample.

[1]

5	

6 A bank has detection software that can be set at two different levels, 'Mild' and 'Severe'.

- When it is set at Mild, 0.1% of all transactions are queried.
- When it is set at Severe 0.5% of all transactions are queried.

(i) One day the bank has 500 000 transactions.

The software is set on 'Mild'. There are 480 false positives. Only $\frac{1}{3}$ of the unauthorised transactions are queried. Complete the table. [3]

(ii) What is the ratio of false positives to false negatives? [1]

(iii) If the software had been set on 'Severe' for the same set of 500 000 transactions, with the total numbers of authorised and unauthorised transactions the same as in part (i) of this question, the number of false negatives would have been 5. What would the ratio of false positives to false negatives have been with this setting? [3]

6 (i)	<table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <thead> <tr> <th style="padding: 5px;">Transactions</th> <th style="padding: 5px;">Authorised</th> <th style="padding: 5px;">Unauthorised</th> <th style="padding: 5px;">Total</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px; text-align: center;">Queried</td> <td style="width: 100px;"></td> <td style="width: 100px;"></td> <td style="width: 100px;"></td> </tr> <tr> <td style="padding: 5px; text-align: center;">Not queried</td> <td></td> <td></td> <td></td> </tr> <tr> <td style="padding: 5px; text-align: center;">Total</td> <td></td> <td></td> <td style="text-align: center;">500 000</td> </tr> </tbody> </table>	Transactions	Authorised	Unauthorised	Total	Queried				Not queried				Total			500 000
Transactions	Authorised	Unauthorised	Total														
Queried																	
Not queried																	
Total			500 000														
6 (ii)	<div style="border: 1px solid black; height: 100px; width: 100%;"></div>																
6 (iii)	<div style="border: 1px solid black; height: 100px; width: 100%;"></div> <p style="text-align: center; margin-top: 10px;">[A copy of the table is provided below for your working.]</p> <table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <thead> <tr> <th style="padding: 5px;">Transactions</th> <th style="padding: 5px;">Authorised</th> <th style="padding: 5px;">Unauthorised</th> <th style="padding: 5px;">Total</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px; text-align: center;">Queried</td> <td style="width: 100px;"></td> <td style="width: 100px;"></td> <td style="width: 100px;"></td> </tr> <tr> <td style="padding: 5px; text-align: center;">Not queried</td> <td></td> <td style="text-align: center;">5</td> <td></td> </tr> <tr> <td style="padding: 5px; text-align: center;">Total</td> <td></td> <td></td> <td style="text-align: center;">500 000</td> </tr> </tbody> </table>	Transactions	Authorised	Unauthorised	Total	Queried				Not queried		5		Total			500 000
Transactions	Authorised	Unauthorised	Total														
Queried																	
Not queried		5															
Total			500 000														

**ADVANCED GCE
MATHEMATICS (MEI)**

4754B

Applications of Advanced Mathematics (C4) Paper B: Comprehension

INSERT

**Monday 13 June 2011
Morning**

Duration: Up to 1 hour

INFORMATION FOR CANDIDATES

- This insert contains the text for use with the questions.
- This document consists of **8** pages. Any blank pages are indicated.

INSTRUCTION TO EXAMS OFFICER / INVIGILATOR

- Do not send this insert for marking; it should be retained in the centre or destroyed.

Card safety

A court case

In a recent (2009) court case, a man claimed that his bank owed him £2100. The money had been taken from his bank account in eight withdrawals from two cash machines, apparently using his bank card, but he said that he had neither made these withdrawals himself nor asked anyone else to make them. His card used chip and PIN technology. The bank had refused to refund his money. 5

The letters PIN stand for Personal Identification Number and refer to a 4-digit number that is needed to authorise transactions using the card, such as withdrawing money. Some banks do not allow numbers that begin with zero, numbers in which the digits are all the same (such as 5555) or numbers in which the digits are consecutive (such as 2345 or 8765). 10

When a bank issues you with a card, various security conditions come with it.

- You are not allowed to tell anyone the PIN.
- You are not allowed to write the PIN down; you must remember it.
- You may not lend the card to anyone else.
- If you lose the card, you must report the loss to the bank. 15

In the 2009 court case, there was no dispute that the withdrawals had taken place. The question was which of the following possible explanations was correct.

1. The man was making a dishonest claim. If so, the man is clearly at fault.
2. The bank had made an error, for example by taking money from this man's account by mistake, and so is at fault. 20
3. A breach of the card's security conditions, as stated above, had allowed a thief to withdraw the money. If so, the man is legally at fault.
4. A thief had been able to withdraw the money without a breach of the card's security conditions. If so, the fault lies with the bank's systems.

Two of these explanations (1 and 3) say that the man is at fault; the other two (2 and 4) put the blame on the bank. 25

Explanations 3 and 4 involve successful 'attacks' by a thief.

The judge decided in favour of the bank. His written judgment caused some people concern. Part of it could be read as meaning that chip and PIN technology is absolutely secure; if so, it would imply that it is impossible for a thief to copy, or 'clone', someone else's card or to break a bank's security. 30

A survey of card users

Following this judgment, MEI conducted a small survey to provide information about the situation, and particularly the four possible explanations. Those taking part were mathematics teachers attending a conference in June 2009; 250 questionnaires were given out and 80 returned. The survey was based on people's experience with their banks. 35

Banks use software designed to detect suspicious transactions; if one is detected, the bank usually contacts the card-holder to check whether the transaction should go ahead. The survey asked people whether they had been contacted by their banks about a suspicious transaction.

If the answer was Yes, they were then asked to answer a further question as to whether they had 40

authorised the transaction. An answer of Yes to this further question meant that the transaction was genuine, and an answer of No that an attack had been detected.

- 46 of the 80 respondents had been contacted by their banks, many of them several times.
- Most of the transactions had in fact been authorised, but 11 of the 46 people had been contacted about unauthorised transactions. 45
- Of the 11 people with unauthorised transactions, 3 could explain them as breaches of card security (typically losing the card) but 9 could not (one person was in both categories).

The survey then went on to ask about cases that had not been picked up by the banks' detection software, resulting in unauthorised withdrawals from people's accounts.

- 21 people reported unauthorised withdrawals. 50
- Of these, 9 people could explain them as breaches of card security and 13 could not (again one person was in both categories).

In total, 16 out of the 80 people who responded to the survey had been the subject of attacks in which there was no breach of the card's security conditions. Some of the attacks had been stopped by their banks but others had resulted in money being withdrawn from their accounts; some people reported both of these. If the survey results are reasonably representative, they would suggest that, in the course of the $3\frac{1}{2}$ years covered by the survey, 20% of people had suffered an attack without any breach of their cards' security. This may be an overestimate. Only 80 out of 250 people returned the questionnaire; maybe all the 170 who did not return it had nothing to report. In that case the proportion suffering such an attack would be 6.4%. 55
60

The conclusion that attacks can happen without breaches of card security is supported by the fact that banks are prepared to bear the considerable costs that must be involved in the process of carrying out checks.

Possible explanations

In a typical court case involving card security, the claimant has had money withdrawn from an account and the bank has refused to refund it. There is no dispute that the withdrawal has taken place. The four possible explanations on the first page apply and the results from the survey make it possible to say something about them. 65

In the first explanation, it is the claimant who has withdrawn the money and is then saying it was someone else. The survey suggests that the other explanations are also possible. Whether the court judges the claimant to be telling the truth must depend on other evidence. 70

The next possible explanation is that the bank made an error, and this can happen. One of the responses to the questionnaire said

“We went to the bank and spoke at length with the manager. We were fully reimbursed and had a grovelling apology.” 75

That leaves the two explanations that involve the money being taken by a thief, with or without a breach of the card's security. The survey also identified the number of transactions, as well as the number of people, subject to attacks. There were a total of 42 attacks; several people reported more than one attack. 13 of the attacks could be explained by breaches of card security and 29 could not.

So the data would suggest that, if there has been an attack, the probabilities of the two explanations of breach and no breach of card security are $\frac{13}{42}$ and $\frac{29}{42}$. These figures are based on a small sample and so it would be better to think of them as about $\frac{1}{3}$ and $\frac{2}{3}$. In civil cases, courts decide the outcome on a 'balance of probabilities'. The probabilities of $\frac{1}{3}$ and $\frac{2}{3}$ are so close together that a court would 80

be unwilling to decide the matter on the basis of them alone, and would look for other evidence before reaching a decision.

85

The banks

The survey went on to ask those who reported unauthorised withdrawals what happened next. In nearly all cases the bank had refunded the money but in one case this had not happened.

One of the responses to the questionnaire said

“The bank described two transactions in the space of 3 or 4 hours. One for about £40 in a shop in London and the other for over £500 at an expensive restaurant/club in London. I was in Paris at the time of these transactions. The bank refunded both amounts after I filled in a form. ... I assume that someone had managed to clone my card somehow.”

90

Clearly fraud can cost the banks a lot of money.

95

If a bank refuses to pay, the next course of action open to someone who has lost money in this way is to contact the independent Financial Ombudsman. A few of these cases are then taken further and end up in court.

Detecting fraud

The survey provided information about the banks' success in detecting unauthorised transactions. The total number of transactions for those who responded has been estimated as 100 000 for the 3½ years covered by the survey. Table 1 shows data from the survey and, in brackets, figures derived from the estimate of 100 000 transactions.

100

Transactions	Authorised	Unauthorised	Total
Queried	139	19	158
Not queried	(99 819)	23	(99 842)
Total	(99 958)	42	(100 000)

Table 1

Table 1 illustrates the problems faced by the banks. They check a very large number of transactions, query quite a small proportion of them and succeed in stopping a small number of unauthorised transactions. However, despite all this effort, the figures in Table 1 suggest that they only catch about half of the attacks.

105

The entries in a table like this are often described using the terms in Table 2.

Transactions	Authorised	Unauthorised
Queried	False positives	True positives
Not queried	True negatives	False negatives

Table 2

A 'positive' is a transaction that is identified by a bank's computer software as suspect and so is queried. The identification is 'false' if the transaction was in fact authorised and it is 'true' if the transaction was unauthorised. 110

Similarly, a 'negative' is a transaction that is not identified as suspect and this non-identification may be true or false.

So, if the software gives a warning when there is no attack, a false positive results; 139 of these are recorded in Table 1 and, apart from some inconvenience, they are quite harmless. If, however, the software fails to give a warning when there really is an attack, a false negative occurs, resulting in unauthorised withdrawals and these are the serious cases; there are 23 of them in Table 1. 115

The number of false negatives can be reduced by making the warning criteria in the software more severe, but the effect will inevitably be that the number of false positives rises: the more severe warning criteria will pick out more authorised transactions. Thus the fewer the false negatives, the greater the number of false positives, and vice-versa. 120

The detection software may be thought of as the front line in the ongoing struggle between thieves and banks. Once thieves learn how it is programmed, they can find ways to defeat it. Consequently the information is considered to be top secret by the banks.

Finally, a piece of advice. Never let anyone else use your card. Legally, your PIN is an electronic signature and so allowing someone else to use it is the equivalent of telling them to forge your signature. 125

BLANK PAGE

BLANK PAGE

**Copyright Information**

OCR is committed to seeking permission to reproduce all third-party content that it uses in its assessment materials. OCR has attempted to identify and contact all copyright holders whose work is used in this paper. To avoid the issue of disclosure of answer-related information to candidates, all copyright acknowledgements are reproduced in the OCR Copyright Acknowledgements Booklet. This is produced for each series of examinations and is freely available to download from our public website (www.ocr.org.uk) after the live examination series.

If OCR has unwittingly failed to correctly acknowledge or clear any third-party content in this assessment material, OCR will be happy to correct its mistake at the earliest possible opportunity.

For queries or further information please contact the Copyright Team, First Floor, 9 Hills Road, Cambridge CB2 1GE.

OCR is part of the Cambridge Assessment Group; Cambridge Assessment is the brand name of University of Cambridge Local Examinations Syndicate (UCLES), which is itself a department of the University of Cambridge.