

2015年6月·第3套 英语六级长篇阅读（信息匹配） 第1篇·36-45 题 答案与解析

STATEMENTS & ANALYSIS • 信息匹配题和解析

信息匹配题和解析·36-45 题

本页 36-45 题的段落匹配答案与逐句解析由懒笔记基于2015年6月·第3套 英语六级长篇阅读（信息匹配）原卷逐题核对整理。与试卷排版同一卷面：先是 Directions 与 15 段字母标号长文（逐段附中文翻译）；之后 10 句陈述逐句排列，每句英文陈述后紧接本句解析——陈述句中译、信息所在段落、锚点强弱、定位句中英对照、陈述句与原文的同义改写对照与易混相邻段辨析。

真题卷第3套(2015-06)·六级

Part III Section B

Directions: In this section, you are going to read a passage with ten statements attached to it. Each statement contains information given in one of the paragraphs. Identify the paragraph from which the information is derived. You may choose a paragraph more than once. Each paragraph is marked with a letter. Answer the questions by marking the corresponding letter on **Answer Sheet 2**.

Plastic Surgery

A better credit card is the solution to ever larger hack attacks.

A) A thin magnetic stripe (magstripe) is all that stands between your credit-card information and the bad guys. And they've been working hard to break in. That's why 2014 is shaping up as a major showdown: banks, law enforcement and technology companies are all trying to stop a network of hackers who are succeeding in stealing account numbers, names, email addresses and other crucial data used in identity theft. More than 100 million accounts at Target, Neiman Marcus and Michaels stores were affected in some way during the most recent attacks, starting last November.

一条薄薄的磁条就是你的信用卡信息与不法分子之间的唯一屏障。而他们一直在努力攻破它。这就是为什么2014年正在形成一场重大对决：银行、执法部门和科技公司都在试图阻止一个黑客网络，这些黑客正成功窃取账号、姓名、电子邮件地址以及其他用于身份盗窃的关键数据。从去年11月开始的最近几次攻击中，Target、Neiman Marcus和Michaels商店超过1亿个账户以某种方式受到了影响。

B) Swipe(刷卡) is the operative word: cards are increasingly vulnerable to attacks when you make purchases in a store. In several recent incidents, hackers have been able to obtain massive information of credit-debit(借记) or prepaid-card numbers using malware, i.e. malicious software, inserted secretly into the retailers' point-of-sale system—the checkout registers. Hackers then sold the data to a second group of criminals operating in shadowy corners of the web. Not long after, the stolen data was showing up on fake cards and being used for online purchases.

刷卡是关键词：当你在商店购物时，银行卡越来越容易受到攻击。在最近的几起事件中，黑客能够通过恶意软件获取大量信用卡、借记卡或预付卡号码信息，这些恶意软件被秘密植入零售商的销售点系

统——收银机。然后黑客将数据出售给在网络阴暗角落活动的第二组犯罪分子。不久之后，被盗数据就出现在伪造卡上，并被用于网上购物。

- C) The solution could cost as little as \$2 extra for every piece of plastic issued. The fix is a security technology used heavily outside the U.S. While American credit cards use the 40-year-old magstripe technology to process transactions, much of the rest of the world uses smarter cards with a technology called EMV (short for Europay, MasterCard, Visa) that employs a chip embedded in the card plus a customer PIN (personal identification number) to authenticate(验证) every transaction on the spot. If a purchaser fails to punch in the correct PIN at the checkout, the transaction gets rejected. (Online purchases can be made by setting up a separate transaction code.)

解决方案可能只需为每张塑料卡额外支付2美元。这一修复方案是一种在美国以外大量使用的安全技术。美国信用卡使用有40年历史的磁条技术来处理交易，而世界其他地区使用一种叫做EMV（Europay、MasterCard、Visa的缩写）的更智能的卡片技术，该技术在卡中嵌入芯片，加上客户PIN码（个人识别码）来即时验证每笔交易。如果购买者在结账时未能输入正确的PIN码，交易就会被拒绝。（网上购物可以通过设置单独的交易代码来完成。）

- D) Why haven't big banks adopted the more secure technology? When it comes to mailing out new credit cards, it's all about relative costs, says David Robertson, who runs the Nilson Report, an industry newsletter. "The cost of the card, putting the sticker on it, coding the account number and expiration date, embossing(凸印) it, the small envelope—all put together, you're in the dollar range." A chip-and-PIN card currently costs closer to \$3, says Robertson, because of the price of chips. (Once large issuers convert together, the chip costs should drop.)

为什么大银行没有采用更安全的技术？行业通讯《Nilson Report》的负责人David Robertson说，当涉及到邮寄新信用卡时，这完全关乎相对成本。“卡片的成本、贴标签、编码账号和到期日期、凸印、小信封——所有这些加在一起，你的成本在1美元范围内。”Robertson说，由于芯片的价格，芯片加PIN码卡目前的成本接近3美元。（一旦大型发卡机构一起转换，芯片成本应该会下降。）

- E) Multiply \$3 by the more than 5 billion magstripe credit and prepaid cards in circulation in the U.S. Then consider that there's an estimated \$12.4 billion in card fraud on a global basis, says Robertson. With 44% of that in the U.S., American credit-card fraud amounts to about \$5.5 billion annually. Card issuers have so far calculated that absorbing the liability for even big hacks like the Target one is still cheaper than replacing all that plastic.

用3美元乘以美国流通的超过50亿张磁条信用卡和预付卡。Robertson说，然后考虑到全球范围内估计有124亿美元的银行卡欺诈。其中44%发生在美国，美国信用卡欺诈每年约达55亿美元。到目前为止，发卡机构计算出，即使像Target这样的大规模黑客攻击，承担责任仍然比更换所有这些塑料卡更便宜。

- F) That leaves American retailers pretty much alone the world over in relying on magstripe technology to charge purchases—and leaves consumers vulnerable. Each magstripe has three tracks of information, explains payments security expert Jeremy Gumbley, the chief technology officer of Credit Call, an electronic-payments company. The first and third are used by the bank or card issuer. Your vital account information lives on the second track, which hackers try to capture. "Malware is

scanning through the memory in real time and looking for data," he says. "It creates a text file that gets stolen."

这使得美国零售商在全世界几乎独自依赖磁条技术来收费购物——并使消费者处于脆弱境地。支付安全专家、电子支付公司Credit Call的首席技术官Jeremy Gumbley解释说，每条磁条有三轨信息。第一轨和第三轨由银行或发卡机构使用。你的重要账户信息存储在第二轨上，黑客试图捕获的就是这一轨。他说："恶意软件实时扫描内存并寻找数据。它创建一个会被盗取的文本文件。"

- G) Chip-and-PIN cards, by contrast, make fake cards or skimming impossible because the information that gets scanned is encrypted(加密). The historical reason the U.S. has stuck with magstripe, ironically enough, is once superior technology. Our cheap, ultra-reliable wired networks made credit-card authentication over the phone frictionless. In France, card companies created EMV in part because the telephone monopoly was so maddeningly inefficient and expensive. The EMV solution allowed transactions to be verified locally and securely.

相比之下，芯片加PIN码卡使伪造卡或盗刷变得不可能，因为被扫描的信息是加密的。具有讽刺意味的是，美国坚持使用磁条的历史原因恰恰是曾经的优越技术。我们廉价、超可靠的有线网络使通过电话进行信用卡验证变得顺畅无阻。在法国，卡公司创建EMV部分是因为电话垄断效率低下且费用高得令人发狂。EMV解决方案允许在本地安全地验证交易。

- H) Some big banks, like Wells Fargo, are now offering to convert your magstripe card to a chip-and-PIN model. It's actually a hybrid(混合体) that will still have a magstripe, since most U.S. merchants don't have EMV terminals. Should you take them up on it? If you travel internationally, the answer is yes.

一些大银行，如Wells Fargo，现在提供将你的磁条卡转换为芯片加PIN码模式。这实际上是一种混合体，仍然会有磁条，因为大多数美国商家没有EMV终端。你应该接受吗？如果你经常出国旅行，答案是肯定的。

- I) Keep in mind, too, that credit cards typically have better liability protection than debit cards. If someone uses your credit card fraudulently(欺诈性的), it's the issuer or merchant, not you, that takes the hit. Debit cards have different liability limits depending on the bank and the events surrounding any fraud. "If it's available, the logical thing is to get a chip-and-PIN card from your bank," says Eric Adamowsky, a co-founder of Credit CardInsider.com. "I would use credit cards over debit cards because of liability issues." Cash still works pretty well too.

还要记住，信用卡通常比借记卡有更好的责任保护。如果有人欺诈性地使用你的信用卡，承担损失的是发卡机构或商家，而不是你。借记卡根据银行和围绕任何欺诈的事件有不同的责任限额。

CreditCardInsider.com的联合创始人Eric Adamowsky说："如果有的话，合乎逻辑的做法是从你的银行获得一张芯片加PIN码卡。由于责任问题，我会使用信用卡而不是借记卡。"现金也仍然很好用。

- J) Retailers and banks stand to benefit from the lower fraud levels of chip-and-PIN cards but have been reluctant for years to invest in the new infrastructure(基础设施) needed for the technology, especially if consumers don't have access to it. It's a chicken-and-egg problem: no one wants to spend the money on upgraded point-of-sale systems that can read the chip cards if shoppers aren't carrying them—yet there's little point in consumers' carrying the fancy plastic if stores aren't equipped to use them.

(An earlier effort by Target to move to chip and PIN never gained progress.) According to Gumbley, there's a "you-first mentality. The logjam(僵局) has to be broken."

零售商和银行可以从芯片加PIN码卡较低的欺诈率中受益，但多年来一直不愿投资于该技术所需的新基础设施，特别是如果消费者无法使用它。这是一个先有鸡还是先有蛋的问题：如果购物者不携带芯片卡，没有人愿意在可以读取芯片卡的升级销售点系统上花钱——但如果商店没有配备使用它们的设备，消费者携带这种高级塑料卡也没有意义。（Target早期向芯片加PIN码转变的努力从未取得进展。）根据Gumbley的说法，存在一种“你先来的心态。僵局必须被打破。”

- K) JPMorgan Chase CEO Jamie Dimon recently expressed his willingness to do so, noting that banks and merchants have spent the past decade suing each other over interchange fees—the percentage of the transaction price they keep—rather than deal with the growing hacking problem. Chase offers a chip-enabled card under its own brand and several others for travel-related companies such as British Airways and Ritz-Carlton.

摩根大通CEO Jamie Dimon最近表示愿意这样做，他指出，银行和商家在过去十年里一直在就交换费——他们保留的交易价格百分比——互相起诉，而不是处理日益严重的黑客问题。Chase在其自有品牌下提供芯片卡，并为British Airways和Ritz-Carlton等旅游相关公司提供其他几种芯片卡。

- L) The Target and Neiman hacks have also changed the cost calculation: although retailers have been reluctant to spend the \$6.75 billion that Capgemini consultants estimate it will take to convert all their registers to be chip-and-PIN-compatible, the potential liability they now face is dramatically greater. Target has been hit with class actions from hacked consumers. "It's the ultimate nightmare," a retail executive from a well-known chain admitted to TIME.

Target和Neiman的黑客攻击也改变了成本计算：尽管零售商一直不愿花费Capgemini咨询公司估计的67.5亿美元来将所有收银机转换为芯片加PIN码兼容，但他们现在面临的潜在责任要大得多。Target已经被遭到黑客攻击的消费者提起集体诉讼。一位知名连锁店的零售高管向TIME承认：“这是终极噩梦。”

- M) The card-payment companies MasterCard and Visa are pushing hard for change. The two firms have warned all parties in the transaction chain—merchant, network, bank—that if they don't become EMV-compliant by October 2015, the party that is least compliant will bear the fraud risk.

银行卡支付公司MasterCard和Visa正在大力推动变革。这两家公司已经警告交易链中的所有各方——商家、网络、银行——如果他们在2015年10月之前不符合EMV标准，合规性最低的一方将承担欺诈风险。

- N) In the meantime, app-equipped smartphones and digital wallets—all of which can use EMV technology—are beginning to make inroads(侵染) on cards and cash. PayPal, for instance, is testing an app that lets you use your mobile phone to pay on the fly at local merchants—without surrendering any card information to them. And further down the road is biometric authentication, which could be encrypted with, say, a fingerprint.

与此同时，配备应用程序的智能手机和数字钱包——所有这些都可以使用EMV技术——正开始侵染银行卡和现金领域。例如，PayPal正在测试一款应用程序，让你可以使用手机在当地商家即时付款——而无需向他们交出任何银行卡信息。而更远的未来是生物识别认证，可以用指纹等进行加密。

- O) Credit and debit cards, though, are going to be with us for the foreseeable future, and so are hackers, if we stick with magstripe technology. "It seems crazy to me," says Gumbley, who is

English, "that a cutting-edge technology country is depending on a 40-year-old technology." That's why it may be up to consumers to move the needle on chip and PIN. Says Robertson: "When you get the consumer into a position of worry and inconvenience, that's where the rubber hits the road."

不过，在可预见的未来，信用卡和借记卡将伴随我们，如果我们坚持使用磁条技术，黑客也会如此。

英国人Gumbley说："在我看来这很疯狂，一个尖端技术国家却依赖40年前的技术。"这就是为什么推动芯片加PIN码可能要靠消费者了。Robertson说："当你让消费者陷入担忧和不便的境地时，那才是关键时刻。"

陈述句与逐句解析

36. It is best to use an EMV card for international travel.

国际旅行最好使用EMV卡。

【答案】 **H** 段（强锚点）

【锚点】 出国旅行（international travel）

【定位】 Should you take them up on it? If you travel internationally, the answer is yes.

你应该接受银行提供的这种升级吗？如果你常出国，答案是肯定的。

【改写】 an EMV card ↔ a chip-and-PIN model

EMV 卡 = 芯片 + PIN 卡（专有术语等价）

international travel ↔ If you travel internationally

international travel 与 travel internationally 词形微变

It is best to use ↔

Should you take them up on it? If you travel internationally, the answer is yes.

‘最好做’与‘问 + 肯定回答’句式等值

【辨邻】 **C** C 段的核心是 much of the rest of the world uses smarter cards with a technology called EMV——是技术定义与现状对比，并没有出现‘出国时应使用’这层建议。它制造的迷惑是‘EMV 一词在此段最显眼’，但并非源头段。

While American credit cards use the 40-year-old magstripe technology to process transactions, much of the rest of the world uses smarter cards with a technology called EMV

37. Personal information on credit and debit cards is increasingly vulnerable to hacking.

信用卡和借记卡上的个人信息越来越容易受到黑客攻击。

【答案】 **B** 段（弱锚点）

【锚点】 信用卡和借记卡上的个人信息 + 越发易受攻击（increasingly vulnerable）

【定位】Swipe(刷卡) is the operative word: cards are increasingly vulnerable to attacks when you make purchases in a store. In several recent incidents, hackers have been able to obtain massive information of credit-debit-(借记) or prepaid-card numbers using malware, i.e. malicious software, inserted secretly into the retailers' point-of-sale system—the checkout registers.

‘刷卡’是关键词：当你在店里付款时，卡正变得越来越容易被攻击。在最近几起事件中，黑客把恶意软件偷偷植入零售商的销售点系统（即收银机），从而批量获取信用卡、借记卡或预付卡的卡号。

【改写】Personal information on credit and debit cards ↔ **credit-debit-(借记) or prepaid-card numbers**
卡号是个人信息的下位实例

increasingly vulnerable to hacking ↔ **cards are increasingly vulnerable to attacks**
increasingly vulnerable 同根近义原样复现

【辨邻】A banks, law enforcement and technology companies are all trying to stop a network of hackers 与 More than 100 million accounts at Target, Neiman Marcus and Michaels stores were affected 的论述焦点是‘反击 + 受害规模’，不是陈述句要求的‘信用卡 + 借记卡上个人信息越来越易被黑’这一直接断言。

banks, law enforcement and technology companies are all trying to stop a network of hackers who are succeeding in stealing account numbers, names, email addresses and other crucial data used in identity theft

F Each magstripe has three tracks of information 的论述是‘磁条物理结构 + 第二轨被攻击’，没有‘越来越脆弱’这层动态判断，也没有 credit + debit 两类卡并列的表述。

Your vital account information lives on the second track, which hackers try to capture

38. The French card companies adopted EMV technology partly because of inefficient telephone service.

法国卡公司采用EMV技术部分是因为电话服务效率低下。

【答案】G 段（强锚点）

【锚点】法国卡公司 + 低效的电话服务

【定位】In France, card companies created EMV in part because the telephone monopoly was so maddeningly inefficient and expensive.

在法国，卡公司之所以创建了 EMV，部分原因是当时的电话垄断公司极其低效和昂贵。

【改写】 The French card companies ↔ **In France, card companies**

形容词形式 vs 介词短语等值

adopted EMV technology ↔ **created EMV**

adopt 与 create 在‘引入新技术’语境下近义

inefficient telephone service ↔

the telephone monopoly was so maddeningly inefficient and expensive

名词短语 vs 表语描述等值

partly because ↔ **in part because**

因果连接词原样近义复现

39. While many countries use the smarter EMV cards, the U.S. still clings to its old magstripe technology.

虽然许多国家使用更智能的EMV卡,但美国仍然坚持使用其旧的磁条技术。

【答案】 **C** 段 (强锚点)

【锚点】 许多国家用 EMV vs 美国仍守磁条

【定位】 While American credit cards use the 40-year-old magstripe technology to process transactions, much of the rest of the world uses smarter cards with a technology called EMV (short for Europay, MasterCard, Visa) that employs a chip embedded in the card plus a customer PIN (personal identification number) to authenticate(验证) every transaction on the spot.

尽管美国的信用卡仍在用 40 年历史的磁条技术处理交易, 但世界其他大多数地区已用上了更智能的卡——这种卡采用一种叫做 EMV 的技术, 靠卡内嵌入的芯片加上消费者的 PIN 码在交易现场验证每一笔交易。

【改写】 many countries use the smarter EMV cards ↔

much of the rest of the world uses smarter cards with a technology called EMV

‘many countries’ ↔ ‘much of the rest of the world’是数量级同义替换

the U.S. still clings to its old magstripe technology ↔

American credit cards use the 40-year-old magstripe technology to process transactions

‘clings to its old magstripe’ ↔ ‘use the 40-year-old magstripe’动词色彩改写

【辨邻】 G The historical reason the U.S. has stuck with magstripe, ironically enough, is once superior technology 论述的是‘美国为何坚守磁条’这一历史原因，而非陈述句所说的‘很多国家用 EMV 而美国仍用磁条’这一现状对比。‘stuck with magstripe’的词面也制造迷惑。

The historical reason the U.S. has stuck with magstripe, ironically enough, is once superior technology

F That leaves American retailers pretty much alone the world over in relying on magstripe technology to charge purchases—and leaves consumers vulnerable——重心在‘让消费者暴露’的后果，没有把 EMV 作为对比的另一极并列出来。

That leaves American retailers pretty much alone the world over in relying on magstripe technology to charge purchases—and leaves consumers vulnerable

40. Attempts are being made to prevent hackers from carrying out identity theft.

人们正在努力防止黑客进行身份盗窃。

【答案】 A 段（弱锚点）

【锚点】 正在做出努力阻止黑客实施身份盗窃

【定位】 That's why 2014 is shaping up as a major showdown: banks, law enforcement and technology companies are all trying to stop a network of hackers who are succeeding in stealing account numbers, names, email addresses and other crucial data used in identity theft.

这就是为什么 2014 年将是一场大对决：银行、执法机构和科技公司都在合力阻止一个黑客网络——这个网络正在成功窃取账户、姓名、邮箱等用于身份盗窃的关键数据。

【改写】 Attempts are being made ↔

banks, law enforcement and technology companies are all trying to stop

被动 ‘Attempts are being made’ 等于多主语主动 ‘are all trying to’

prevent hackers from carrying out identity theft ↔

stop a network of hackers who are succeeding in stealing account numbers, names, email addresses and other crucial data used in identity theft

prevent...from doing ↔ stop...who are doing 等值

【辨邻】 M The card-payment companies MasterCard and Visa are pushing hard for change 的‘push for change’是机制层面的‘推动转换’，未直接陈述‘阻止黑客实施身份盗窃’，且不含 identity theft 一词。

The card-payment companies MasterCard and Visa are pushing hard for change

41. Credit cards are much safer to use than debit cards.

信用卡比借记卡使用起来安全得多。

【答案】 I 段（强锚点）

【锚点】 信用卡比借记卡安全得多

【定位】 Keep in mind, too, that credit cards typically have better liability protection than debit cards.
也请记住，信用卡通常比借记卡有更好的赔付责任保护。

【改写】 Credit cards are much safer to use than debit cards ↔

credit cards typically have better liability protection than debit cards

‘safer’与‘better liability protection’是上位 vs 具体的同义改写

much safer ↔ **I would use credit cards over debit cards because of liability issues**

‘much safer’得到原文专家偏好语的支撑

【辨邻】 B credit-debit-(借记) or prepaid-card numbers 把两类卡并列只是为说明‘黑客可同时窃取两类卡的卡号’，没有对比 credit 和 debit 的安全性高低。

hackers have been able to obtain massive information of credit-debit-(借记) or prepaid-card numbers

42. Big banks have been reluctant to switch to more secure technology because of the higher costs involved.

大型银行一直不愿转向更安全的技术,因为涉及更高的成本。

【答案】 D 段 (强锚点)

【锚点】 大银行不愿换 + 因为成本更高

【定位】 Why haven't big banks adopted the more secure technology? When it comes to mailing out new credit cards, it's all about relative costs, says David Robertson, who runs the Nilson Report, an industry newsletter.

为什么大银行还没采用更安全的技术? David Robertson (行业通讯 Nilson Report 的负责人) 说, 谈到寄出新信用卡, 归根结底是相对成本的问题。

【改写】 Big banks have been reluctant to switch ↔

Why haven't big banks adopted the more secure technology?

‘haven't adopted’与‘reluctant to switch’行为 ↔ 心理同义

because of the higher costs involved ↔ **it's all about relative costs**

‘relative costs’对应‘higher costs’的具体落点

more secure technology ↔ **the more secure technology**

原样复现

【辨邻】 E Card issuers have so far calculated that absorbing the liability for even big hacks like the Target one is still cheaper than replacing all that plastic 是结论性总账，不是大银行迟迟不换的直接原因表述；陈述句问的是‘为何不愿换’，E 段答的是‘吸收欺诈仍便宜’的衡量结果。

Card issuers have so far calculated that absorbing the liability for even big hacks like the Target one is still cheaper than replacing all that plastic

J Retailers and banks stand to benefit from the lower fraud levels of chip-and-PIN cards but have been reluctant for years to invest in the new infrastructure(基础设施) needed for the technology 谈的是双方互推投资意愿，与陈述句的‘大银行 + 成本 + 不愿换卡’这一单方面因果不对应。

have been reluctant for years to invest in the new infrastructure(基础设施) needed for the technology

43. The potential liability for retailers using magstripe is far more costly than upgrading their registers.

零售商使用磁条卡的潜在责任远比升级其收银机的成本高得多。

【答案】 L 段（强锚点）

【锚点】 零售商用磁条的潜在赔付风险 vs 升级收银机成本

【定位】 The Target and Neiman hacks have also changed the cost calculation: although retailers have been reluctant to spend the \$6.75 billion that Capgemini consultants estimate it will take to convert all their registers to be chip-and-PIN-compatible, the potential liability they now face is dramatically greater.

Target 和 Neiman 两起入侵事件也改变了成本账：尽管零售商一直不情愿花费 Capgemini 顾问估算的 67.5 亿美元改造所有收银机以兼容芯片 + PIN，但他们现在面临的潜在赔付风险已远远更大。

【改写】 The potential liability for retailers using magstripe ↔

the potential liability they now face is dramatically greater

potential liability 原样复现

far more costly than upgrading their registers ↔

\$6.75 billion that Capgemini consultants estimate it will take to convert all their registers to be chip-and-PIN-compatible

‘upgrade registers’对应‘convert all their registers to be chip-and-PIN-compatible’的概括等值

【辨邻】 D A chip-and-PIN card currently costs closer to \$3 与 you're in the dollar range 的对比是单卡 3 vs 1，与陈述句的‘潜在赔付 vs 升级收银机’不在同一对比维度。

A chip-and-PIN card currently costs closer to \$3

E Card issuers have so far calculated that absorbing the liability for even big hacks like the Target one is still cheaper than replacing all that plastic 是发卡方角度的‘吸收赔付便宜’，主体与陈述句的零售商不同，结论方向也相反，正话反说陷阱。

absorbing the liability for even big hacks like the Target one is still cheaper than replacing all that plastic

44. The use of magstripe cards by American retailers leaves consumers exposed to the risks of losing account information.

美国零售商使用磁条卡使消费者面临账户信息丢失的风险。

【答案】 F 段（弱锚点）

【锚点】 美国零售商用磁条 + 让消费者面临账户信息泄露风险

【定位】 That leaves American retailers pretty much alone the world over in relying on magstripe technology to charge purchases—and leaves consumers vulnerable.

这让美国零售商在全世界范围内几乎成了仍然依赖磁条技术收款的孤例，也让消费者暴露在风险之中。

【改写】 The use of magstripe cards by American retailers ↔

American retailers pretty much alone the world over in relying on magstripe technology to charge purchases

名词化短语 vs 动词化原文等值

leaves consumers exposed to the risks of losing account information ↔

leaves consumers vulnerable

‘exposed to the risks of losing account information’ ↔ ‘vulnerable + 下文账户信息被捕’上位 vs 具体的对应

【辨邻】 B hackers have been able to obtain massive information of credit-debit-(借记) or prepaid-card numbers using malware 论述的是入侵路径，主语是 hackers；陈述句要求主语是 American retailers 的‘使用磁条’行为导致‘消费者暴露’，方向不一致。

hackers have been able to obtain massive information of credit-debit-(借记) or prepaid-card numbers using malware, i.e. malicious software, inserted secretly into the retailers' point-of-sale system

C While American credit cards use the 40-year-old magstripe technology to process transactions 仅停在现状对比，没有把后果落到‘消费者暴露于账户信息丢失’上。

While American credit cards use the 40-year-old magstripe technology to process transactions

45. Consumers will be a driving force behind the conversion from magstripe to EMV technology.

消费者将成为从磁条技术转向EMV技术的推动力量。

【答案】 O 段（强锚点）

【锚点】 消费者将成为从磁条转向 EMV 的推动力

【定位】 That's why it may be up to consumers to move the needle on chip and PIN.

这就是为什么推动芯片 + PIN 普及的关键可能要落在消费者身上。

【改写】 Consumers will be a driving force ↔

it may be up to consumers to move the needle on chip and PIN

'be up to X' ↔ 'X will be a driving force'同义改写

the conversion from magstripe to EMV technology ↔ **chip and PIN**

'from magstripe to EMV' ↔ 'chip and PIN'专有术语等价

Consumers ↔

When you get the consumer into a position of worry and inconvenience, that's where the rubber hits the road

进一步佐证：原文以‘消费者陷入担忧时才会真正发生’再次锁定消费者为关键推动者

【辨邻】 M The card-payment companies MasterCard and Visa are pushing hard for change 把推动者定为卡公司，与陈述句的‘消费者’主体不一致。

The card-payment companies MasterCard and Visa are pushing hard for change

K JPMorgan Chase CEO Jamie Dimon recently expressed his willingness to do so 把率先动作的主体定为银行 CEO，与陈述句的‘消费者’主体不一致。

JPMorgan Chase CEO Jamie Dimon recently expressed his willingness to do so

PARAGRAPH MAP • 段落主旨图

15 个段落各讲了什么

逐段一句主旨 + 该段最具区分度的「信息指纹」，是逐句回扫定位的工作台。

A 开篇定调：磁条卡安全岌岌可危，2014 年银行、执法机构和科技公司联手反击窃取账户信息的黑客网络，并列举了 Target、Neiman Marcus、Michaels 等大规模被攻击事件。

信息指纹 磁条 + 反击黑客网络 + 三大零售商被攻

B 聚焦刷卡环节：黑客把恶意软件植入收银机的销售点系统，批量窃取借记卡、预付卡号，再卖给地下买家用于伪卡或网购。

信息指纹 刷卡 + 恶意软件入侵 POS + 数据转卖

C 给出解决方案：用美国之外广泛使用的 EMV 芯片 + PIN 技术替换 40 年历史的磁条技术，每笔交易由芯片和密码当场验证。

信息指纹 美国仍用 40 年老磁条 vs 世界用 EMV 芯片 + PIN

D 解释大银行为何迟迟不换：成本账。磁条卡每张约 1 美元，芯片 + PIN 卡接近 3 美元，仅芯片就贵很多。

信息指纹 大银行不换是因为芯片卡更贵（约 3 美元 vs 1 美元）

E 继续算账：全美 50 亿张磁条卡 × 3 美元，与全球 124 亿美元、美国 55 亿美元的卡欺诈损失对比，发卡方判断目前承担欺诈损失仍比全员换卡便宜。

信息指纹 5 亿张卡换卡成本 vs 美国 55 亿美元年欺诈损失

F 美国零售商在全球范围内孤独地坚守磁条技术，使消费者暴露在风险中。专家解释磁条三条信息轨道中第二条承载关键账户信息，正是黑客目标。

信息指纹 美国零售商孤独使用磁条让消费者暴露 + 磁条三条轨道第二条最关键

G 对比解释为何美国坚守磁条：因为早年美国电话网络又便宜又可靠，电话授权交易很方便；而法国当年电话垄断低效昂贵，反而催生了 EMV 本地验证方案。

信息指纹 法国电话垄断低效催生 EMV + 美国靠优秀电话网坚守磁条

H 落到操作建议：大银行已开始把磁条卡转换为芯片 + PIN 混合卡（仍带磁条以兼容美国本土商家）；若你常出国，应接受这种升级。

信息指纹 出国旅行应接受芯片 + PIN 混合卡

I 进一步建议：信用卡通常比借记卡有更好的赔付保护；若信用卡被欺诈，承担损失的是发卡方或商家而非消费者；借记卡赔付限额因银行和事件而异。

信息指纹 信用卡的赔付保护比借记卡更好

J 零售商与银行多年不愿投入新基础设施：商家说没人持芯片卡升级 POS 无意义、消费者说没商家受理持卡也没用，形成‘先有鸡还是先有蛋’的僵局。

信息指纹 鸡生蛋蛋生鸡僵局 + 你先来心态

K 摩根大通 CEO Jamie Dimon 表态愿率先推进，并指出过去十年银行与商家忙着为刷卡手续费打官司，反而没解决黑客问题；该行已发行芯片卡，含与英航、丽思卡尔顿等合作品牌。

信息指纹 摩根大通 CEO 表态愿带头 + 手续费打官司分散注意力

L Target 和 Neiman 被黑后成本账翻转：虽然把所有收银机改造为兼容芯片 + PIN 估计要 67.5 亿美元，但零售商现在面临的潜在赔付风险远比这笔钱可怕。

信息指纹 67.5 亿美元改造费 vs 更可怕的潜在赔付 + 集体诉讼

M 万事达和 Visa 强力推动转换：警告交易链上各方（商家、网络、银行）若 2015 年 10 月前不达到 EMV 合规标准，则合规最差的一方将承担欺诈风险。

信息指纹 万事达和 Visa 设 2015 年 10 月期限并将欺诈责任压给最不合规方

N 前瞻：用 EMV 技术的智能手机 App 和数字钱包开始侵蚀刷卡和现金，PayPal 已在测试用手机就近付款且不交出卡号；更远还有指纹等生物识别。

信息指纹 手机 App、数字钱包、PayPal、指纹等生物识别

O 结尾点题：信用卡和借记卡短期内不会消失，黑客也不会消失；要打破僵局，最终可能要靠消费者——当消费者陷入担忧和不便时，事情才会真正推动。

信息指纹 推动转换的最终力量可能是消费者

SENTENCE INSIGHTS • 句子精讲

13 句真题句逐层精讲

下列真题句各有独立的句子解析页——中文翻译、结构树逐层拆解、成分与时态、考点讲解与真题高频词。点击句子进入完整解析。

While American credit cards use the 40-year-old magstripe technology to process transactions, much of the rest of the world uses smarter cards with a technology called EMV (short for Europay, MasterCard, Visa) that employs a chip embedded in the card plus a customer PIN (personal identification number) to authenticate(验证) every transaction on the spot.

C段，第3句

While引导的对比状语从句 + 主句 + 嵌套定语从句的结构，是四六级和考研阅读中高频出现的典型长难句模式。对比结构用于陈述事实差异、定语从句用于补充技术细节，这种组合在科技类、社会类文章中极为常见，掌握后可大量迁移到真题句式。

(Online purchases can be made by setting up a separate transaction code.)

C段，第5句

情态动词加被动语态是四六级和考研阅读中的高频句式，常用于说明某事可以或应当如何完成，本句结构具有较强的代表性，掌握后可迁移到大量类似表达

With 44% of that in the U.S., American credit-card fraud amounts to about \$5.5 billion annually.

E段，第3句

简单句 + 句首状语 + 主谓宾结构是四六级和考研阅读中的常见句式，尤其是描述统计数据 and 事实陈述的场景。短语动词 "amounts to" 和介词短语作状语的用法都有一定代表性。但本句缺少从句和复杂修饰，作为典型句式的代表性不如包含定语从句或状语从句的长难句，因此典型性为中等偏上。

Chip-and-PIN cards, by contrast, make fake cards or skimming impossible because the information that gets scanned is encrypted(加密).

G段，第1句

主句+原因状语从句+定语从句嵌套是四六级和考研阅读中的高频句式，'make+宾语+形容词'结构和被动语态也是常考点，结构代表性较强

Should you take them up on it?

H段，第3句

覆盖主语、谓语、宾语、状语四种核心成分；短语动词 "take up" 和介词短语 "on it" 的边界划分是实用易错点，适合练习成分拆解；但成分种类不够丰富（无定语、补语、表语等）

If someone uses your credit card fraudulently(欺诈性的), it's the issuer or merchant, not you, that takes the hit.

I段，第2句

主句的强调句型 It is...that 结构是重要的语法考点,从句包含完整的主谓宾状结构,主句中还有插入成分 not you 用于对比强调,涵盖了强调句识别、插入语处理、系表结构分析等多个训练点,成分种类丰富且有实用价值

The Target and Neiman hacks have also changed the cost calculation: although retailers have been reluctant to spend the \$6.75 billion that Capgemini consultants estimate it will take to convert all their registers to be chip-and-PIN-compatible, the potential liability they now face is dramatically greater.

L段，第1句

该句是长难句分析的范本，其嵌套深度和逻辑连接词的运用非常均衡，适合作为中高级语法训练的重点突破对象。

PayPal, for instance, is testing an app that lets you use your mobile phone to pay on the fly at local merchants—without surrendering any card information to them.

N段，第2句

成分种类丰富:涵盖主谓宾基本结构、定语从句、方式状语、复合宾语(let sb do)、不定式作目的状语等多种成分。定语从句中关系代词 that 作主语的用法、let 的复合宾语结构、破折号后状语的识别都是值得练习的点,适合作为综合性成分划分练习句。

"It seems crazy to me," says Gumbley, who is English, "that a cutting-edge technology country is depending on a 40-year-old technology."

O段，第2句

涵盖了主谓宾结构、主系表结构、形式主语与真正主语分离、定语从句、主语从句、倒装等多种成分和句式，且直接引语作宾语、关系代词充当主语等都是值得练习的典型考点

That's why it may be up to consumers to move the needle on chip and PIN.

O段，第3句

主系表结构加表语从句是四六级和考研阅读中的高频句式，why 引导表语从句表示原因也是常见用法，形式主语 it 配合不定式是典型搭配，该句结构具有较强代表性和迁移价值。

Says Robertson: "When you get the consumer into a position of worry and inconvenience, that's where the rubber hits the road."

0段，第4句

覆盖引述倒装、时间状语从句、表语从句、主系表结构、get 使役用法、介词短语作状语等多种成分类型，且 that 指代、where 双重功能、习语结构等都是易错点，适合综合练习。

While many countries use the smarter EMV cards, the U.S. still clings to its old magstripe technology.

第39题 题干

"While" 引导的让步或对比状语从句 + 主句，是四六级和考研阅读中的高频句式，常用于表达对比或转折逻辑。掌握这种结构后，学生可在大量真题句中复用识别方法，迁移价值高。

Attempts are being made to prevent hackers from carrying out identity theft.

第40题 题干

被动语态 + 不定式作目的状语是四六级和考研阅读中的高频句式，尤其在科技、社会问题类文章中常见。掌握后可迁移到大量类似句子，具有较高的典型性。

HIGH-FREQUENCY • 真题高频词

本篇出现的 126 个英语六级真题高频词

下列单词既在本篇真题中出现，又是 **英语六级** 历年真题的高频词（在该考试真题中出现的句子数均不少于 8）。每个词标注本篇 出现次数与该考试真题句频，点击可查看该词的释义、音标、词形与真题例句。

magstripe C1

n. 磁条

本篇13次 · 真题 13 句

credit B1

n. 赊购，赊账

本篇12次 · 真题 54 句

consumer B1

n. 消费者

本篇8次 · 真题 165 句

transaction B2

n. 交易

本篇7次 · 真题 9 句

retailer

B2

n. 零售商

本篇6次·真题32句

chip

A2

n. 炸薯条

本篇6次·真题17句

hacker

B2

n. 黑客 (非法入侵计算机系统者)

本篇6次·真题17句

account

A2

n. 账户

本篇5次·真题93句

target

B1

n. 目标,靶子

本篇5次·真题26句

billion

B1

num. 十亿 (1,000,000,000)

本篇4次·真题74句

purchase

B1

v. 购买

本篇4次·真题55句

hack

B2

v. 非法侵入 (计算机系统)

本篇4次·真题8句

solution

B1

n. 解决办法

本篇3次·真题76句

network

B1

n. 网络

本篇3次·真题53句

vulnerable

C1

adj. 易受伤害的

本篇3次·真题30句

attack

A2

v. 攻击

本篇3次·真题28句

convert

B2

v. 转变

本篇3次·真题15句

reluctant

B2

adj. 不情愿的

本篇3次·真题15句

register

B1

v. 登记, 注册

本篇3次·真题9句

better

A1

adj. 更好的 (good 的比较级)

本篇2次·真题205句

data B1

n. 数据

本篇2次 · 真题 181 句

system A2

n. 系统

本篇2次 · 真题 176 句

risk A2

n. 风险

本篇2次 · 真题 167 句

issue B1

n. 问题

本篇2次 · 真题 158 句

online A2

adj. 在线的

本篇2次 · 真题 139 句

potential B2

adj. 潜在的

本篇2次 · 真题 92 句

increasingly B2

adv. 越来越;日益;不断增加地

本篇2次 · 真题 78 句

code B1

n. 代码

本篇2次 · 真题 50 句

track A2

n. 小路

本篇2次 · 真题 48 句

adopt B1

v. 采纳

本篇2次 · 真题 46 句

identity B2

n. 身份

本篇2次 · 真题 39 句

estimate B2

v. 估计

本篇2次 · 真题 36 句

datum C1

n. 数据 (单数形式, 复数为 data)

本篇2次 · 真题 34 句

chain B1

n. 链条

本篇2次 · 真题 32 句

security B1

n. 安全

本篇2次 · 真题 31 句

secure B2

adj. 安全的

本篇2次 · 真题 20 句

cash A2

n. 现金

本篇2次 · 真题 18 句

upgrade B2

v. 升级

本篇2次 · 真题 14 句

scan B1

v. 仔细查看、审视

本篇2次 · 真题 9 句

inefficient B2

adj. 效率低的

本篇2次 · 真题 8 句

would A1

aux. (will 的过去式) 将要, 会

本篇1次 · 真题 568 句

benefit B1

n. 好处

本篇1次 · 真题 244 句

actually A2

adv. 实际上, 事实上 (用于纠正或补充信息)

本篇1次 · 真题 182 句

accord C1

n. (国家、团体间的) 协议

本篇1次 · 真题 167 句

local A2

adj. 当地的

本篇1次 · 真题 143 句

global B2

adj. 全球的

本篇1次 · 真题 140 句

million A2

num. 一百万

本篇1次 · 真题 126 句

process B1

n. 过程

本篇1次 · 真题 126 句

decade B1

n. 十年

本篇1次 · 真题 120 句

affect B1

v. 影响

本篇1次 · 真题 116 句

expert B1

n. 专家

本篇1次 · 真题 114 句

major B1

adj. 主要的

本篇1次 · 真题 108 句

access B1

n. 进入

本篇1次·真题 101 句

event A2

n. 事件

本篇1次·真题 99 句

least A2

det. 最少的

本篇1次·真题 98 句

gain B1

v. 获得;赢得

本篇1次·真题 96 句

customer A2

n. 顾客, 客户

本篇1次·真题 87 句

amount A2

n. 数量

本篇1次·真题 84 句

involve B1

v. 包含

本篇1次·真题 82 句

further B1

adv. 更远地

本篇1次·真题 79 句

recently A2

adv. 最近

本篇1次·真题 76 句

digital B1

adj. 数字的

本篇1次·真题 72 句

available A2

adj. 可获得的

本篇1次·真题 63 句

email A2

n. 电子邮件

本篇1次·真题 53 句

operate B1

v. 运转

本篇1次·真题 52 句

limit B1

n. 限度

本篇1次·真题 51 句

rely B1

v. 依赖;依靠

本篇1次·真题 51 句

range B1

n. 范围

本篇1次·真题 50 句

invest B2

v. 投资 (金钱、时间等以期获得回报)

本篇1次 · 真题 45 句

charge B1

v. 收费

本篇1次 · 真题 44 句

smartphone B1

n. 智能手机

本篇1次 · 真题 44 句

currently B1

adv. 目前, 当前

本篇1次 · 真题 42 句

protection B1

n. 保护

本篇1次 · 真题 42 句

replace A2

v. 替换, 更换 (用新的代替旧的)

本篇1次 · 真题 42 句

attempt B1

v. 试图

本篇1次 · 真题 39 句

basis B2

n. 基础;根据

本篇1次 · 真题 37 句

brand B1

n. 品牌, 商标

本篇1次 · 真题 37 句

retail B2

n. 零售

本篇1次 · 真题 37 句

app B1

n. 应用程序

本篇1次 · 真题 36 句

instance B2

n. 例子

本篇1次 · 真题 35 句

extra A2

adj. 额外的

本篇1次 · 真题 33 句

executive B2

n. 主管;经理;管理人员

本篇1次 · 真题 32 句

firm B1

adj. 坚固的

本篇1次 · 真题 32 句

historical B2

adj. 历史的

本篇1次 · 真题 32 句

massive B2

adj. 巨大的, 大量的

本篇1次·真题 31 句

switch A2

v. 转换

本篇1次·真题 31 句

employ B1

v. 雇用

本篇1次·真题 30 句

spot A2

n. 地点

本篇1次·真题 30 句

obtain B2

v. 获得

本篇1次·真题 29 句

vital B2

adj. 极其重要的, 必不可少的

本篇1次·真题 29 句

relative B1

n. 亲戚, 亲属

本篇1次·真题 26 句

typically B1

adv. 通常, 一般

本篇1次·真题 26 句

web A2

n. 网站

本篇1次·真题 26 句

driving A2

n. 驾驶

本篇1次·真题 25 句

contrast B2

n. 对比

本篇1次·真题 24 句

fee B1

n. 费用

本篇1次·真题 24 句

payment B1

n. 支付

本篇1次·真题 24 句

software B1

n. 软件 (计算机程序)

本篇1次·真题 24 句

chief B1

n. 首领

本篇1次·真题 23 句

admit B1

v. 承认 (事实、错误等)

本篇1次·真题 22 句

mobile B1

adj. 可移动的

本篇1次 · 真题 22 句

crucial B2

adj. 至关重要的

本篇1次 · 真题 21 句

percentage B1

n. 百分比, 百分率

本篇1次 · 真题 21 句

reject B2

v. 拒绝接受

本篇1次 · 真题 20 句

capture B1

v. 捕获

本篇1次 · 真题 19 句

superior B2

adj. 更好的

本篇1次 · 真题 19 句

ultimate B2

adj. 最终的

本篇1次 · 真题 19 句

heavily B1

adv. 大量地

本篇1次 · 真题 18 句

partly B1

adv. 部分地

本篇1次 · 真题 18 句

infrastructure C1

n. 基础设施

本篇1次 · 真题 17 句

costly B2

adj. 昂贵的, 代价高的

本篇1次 · 真题 16 句

dramatically B2

adv. 显著地

本篇1次 · 真题 16 句

guy A2

n. 男人

本篇1次 · 真题 16 句

surround B1

v. 围绕

本篇1次 · 真题 16 句

absorb B2

v. 吸收 (液体、气体等)

本篇1次 · 真题 15 句

plus A2

prep. 加, 加上

本篇1次 · 真题 14 句

calculate B1

v. 计算

本篇1次 · 真题 13 句

equip B1

v. 装备

本篇1次 · 真题 13 句

willingness B2

n. 愿意

本篇1次 · 真题 12 句

fancy B1

v. 想要

本篇1次 · 真题 11 句

file A2

n. 文件

本篇1次 · 真题 11 句

multiply B1

v. 乘

本篇1次 · 真题 11 句

circulation B2

n. 循环

本篇1次 · 真题 10 句

criminal B1

n. 罪犯

本篇1次 · 真题 9 句

shopper A2

n. 购物者

本篇1次 · 真题 9 句

calculation B2

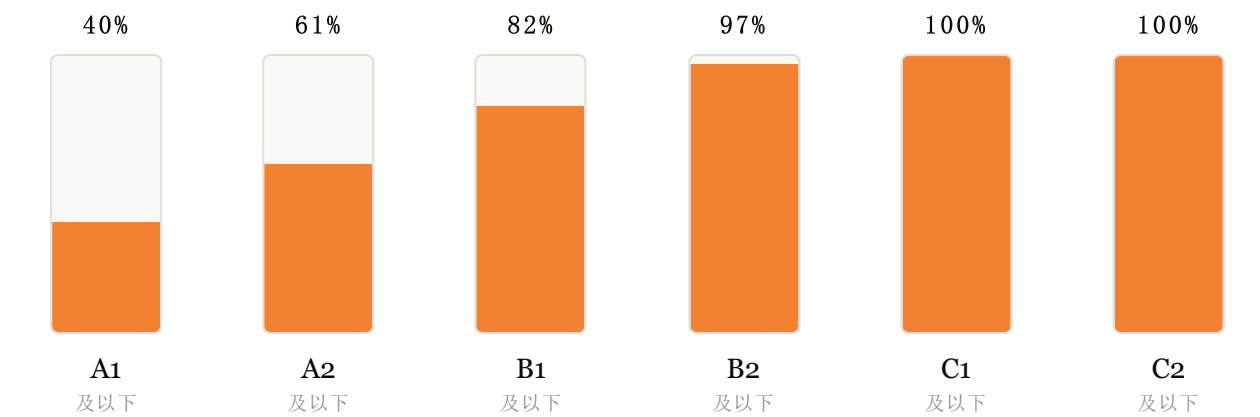
n. 计算

本篇1次 · 真题 8 句

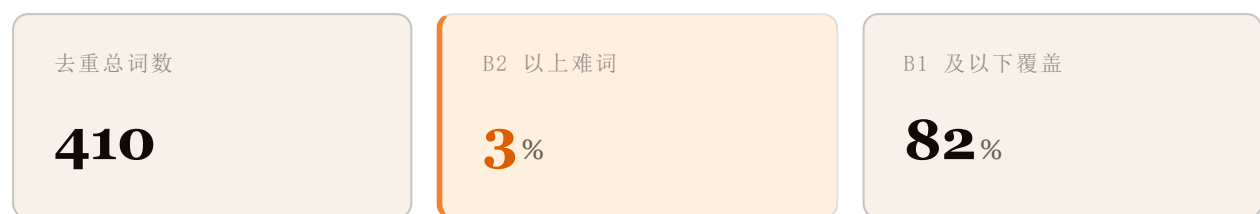
VOCABULARY · 词汇难度分布

全文 410 词按 CEFR 难度累积覆盖

全文去重后共 410 个单词，按欧框 CEFR 等级统计。每根柱表示「该等级及以下」的累积占比（CDF），最右一柱为 100%。B2 以上（C1/C2）为高阶词，本篇共 13 个 · 约 3%。



每柱为「按 CEFR 等级及以下」的累积覆盖率 (CDF) · 数据为全文去重词 410 个 · 末柱为 100%



英语六级 2015年6月·第3套 · 全卷构成

Part I	写作	题目解析 →
Part II	听力	题目解析 →
Part III Section A	完形填空（选词填空）	题目解析 →
Part III Section B	长篇阅读（信息匹配）	本题
Part III Section C (1)	阅读理解（四选一）	题目解析 →
Part III Section C (2)	阅读理解（四选一）	题目解析 →
Part IV	汉译英（段落翻译）	题目解析 →