

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.
- 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.
- 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.)
- 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.)
- 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.
- 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."

- 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.
- 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.
- 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.
- 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."
- 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.
- 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.
- 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.
- 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.

- 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."

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

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

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

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

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

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

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

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

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

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