FDIC Consumer News
Winter 2018

Protecting Your Assets

Tips on Financial Crimes, Mobile Banking and Raising Your Credit Score

Safety Precautions as You Bank on the Go

Guarding Against Card Reader "Skimming" Frauds

Safe Deposit Boxes, Home Safes and Your Valuables

Why Fixing Errors in Credit Reports Can Reduce Loan Interest Rates

Property Appraisals and Mortgage Borrowers

A Closer Look at Mobile Banking: More Uses, More Users

What's new, how you can benefit, and how to protect yourself from security risks

With advances in technology, financial institutions are now increasingly providing customers the ability to use mobile phones for banking transactions and to pay for just about anything from a retail purchase to a restaurant bill you're splitting with friends. "Mobile phones provide opportunities for consumers to conduct their banking transactions and make payments from anywhere at any time," said FDIC Senior Technology Specialist Deborah Shaw. "This is a convenient and beneficial way for consumers to incorporate banking and shopping into their busy lives."

Additionally, FDIC research reported in 2016 showed great potential for mobile financial services to help "underserved" consumers obtain more control over their funds and better manage their bank accounts. The FDIC defines underserved consumers as either "unbanked" (they do not have an account at a federally insured financial institution) or "underbanked" (they have an account at a banking institution but they also obtain financial products and services outside of the banking system, such as check-cashing services). The study, "Opportunities for Mobile Financial Services to Engage Underserved Consumers," is on the FDIC website at www.fdic.gov/consumers/community/mobile/mfs_qualitative_research_report.pdf.

Consumer concerns about safety and security, however, continue to be cited in Federal Reserve Board (Fed) annual reports on mobile financial services (most recently from 2016) as reasons some people do not sign up. Here is the latest overview from ***FDIC Consumer News*** to help consumers better understand the current state of mobile financial services, how they might benefit, and how they can protect themselves against security risks.

Mobile Banking

While many people access their bank accounts by going to their bank, using the telephone or an ATM, or accessing services online with their personal computer, consumers are increasingly using their mobile banking options. That might involve text messaging the bank, accessing a bank's website, or using mobile applications (apps) to check account balances, retrieve account information or initiate financial transactions.

The Fed survey found that 43 percent of all mobile phone users with bank accounts had used mobile banking in the previous 12 months, up from 22 percent in the agency's 2011 survey. Among mobile banking users with smartphones (cell phones with internet connectivity), 53 percent with bank accounts used mobile banking in the previous 12 months.

"A mobile banking application makes it easy to transfer funds within your bank, perhaps to send money to a child's account there or to confirm if you have enough funds to make a purchase or pay a bill," added Ben Navarro, a policy analyst at the FDIC. "The mobile banking app can also often be used for payments across banks."

Mobile banking also can assist consumers in making informed decisions. According to the Fed survey, 62 percent of mobile banking users checked their account balance on their phone before making a large purchase in the store, and 50 percent decided not to purchase an item as a result of their account balance or credit limit.

As previously reported, consumers also can conveniently deposit checks from practically anywhere by transmitting an electronic image of each check and relevant information (see the Summer 2016 ***FDIC Consumer News*** at www.fdic.gov/consumers/consumer/news/cnsum16/photos.html). Many consumers also are using high-tech wristwatches (called "smartwatches") to read bank alerts or to make purchases applied to their credit, debit or prepaid cards (the latter have money deposited on them but they are not linked to a checking or savings account). Ask your bank what services might be available.

And at the FDIC, we've been exploring the potential for mobile banking and mobile payments to bring more low- and moderate-income Americans into the financial mainstream. Recent FDIC surveys have shown that more than one in four households are either unbanked or underbanked.

Additional research by the FDIC showed that one-third of underbanked households used mobile banking in the previous 12 months, and one in eight used it as their primary banking method. The findings suggest that the unbanked and underbanked consumers are attracted to the convenience of

mobile technology and the improved sense of control it provides.

Mobile Payments

For years, consumers have been using smartphones to make purchases at retailers' sales terminals and person-to-person or "P2P" payment services (mobile apps) to conduct everyday payment transactions among family or friends without exchanging cash or a check.

"One of the benefits of mobile P2P apps is that payments are typically initiated on a mobile device using the recipient's smartphone number or email address," Shaw noted. "In this way, a consumer does not have to give the recipient a bank account or card number in order to make a payment; this information remains behind the scenes."

What's changing recently is that there are increasingly more P2P mobile apps being offered by banks and nonbanks that provide consumers many choices. These apps are going beyond personal payments and including broader options for paying for goods and services at stores and other businesses. In 2017, banks began to offer a new service that enables U.S. mobile banking consumers to send funds from one bank account to another in minutes, using only a recipient's email address or mobile number on a mobile banking app. Some of these services offer recipients quicker access to their received (deposited) funds, typically within minutes during business days.

Security Tips

Here are some suggestions to help consumers be safe and secure as they use mobile banking and payment products and services:

Be proactive in how you protect the data on your mobile devices. Start by using "strong" passwords and PINs. If you're given the option to use more than your username and password to access your bank account or mobile apps on your phone – for example, if you can choose to receive a one-time passcode by email or text message that also will be needed to access a certain account or app – that will provide added security.

Avoid using an unsecured Wi-Fi network, often found in public places, such as coffee shops, because fraudsters might be able to access the information you are transmitting or viewing. Log out of your bank account or mobile app when it's not in use. Just like with your laptop, use a mobile security/anti-virus software and keep it updated.

Take additional precautions in case your device is misplaced, lost or stolen. Set the screen on your mobile phone to lock after a certain amount of time and use a PIN or password and/or a biometric indicator (for example, a fingerprint or facial recognition) to unlock your mobile phone. Likewise, use PINs or other security features enabled on your smartwatch, such as one that will lock the watch if it is not on your wrist or too far from your mobile phone. Don't store your PINs or passwords on your mobile phone or tape it to the underside of your smartwatch or mobile phone.

Consider signing up for transaction alerts from your credit card, bank and mobile app provider. These messages can help you identify unauthorized activity quickly. Alternatively, check your transactions regularly on your cards, bank account and mobile app website.

Research any mobile app before downloading and using it. "Make sure you are comfortable that the mobile app is from a reputable source," said Shaw. "Going to the bank's or company's website to find directions for downloading their app can help to ensure you are downloading a legitimate app."

Be on guard against fraudulent emails or text messages. These communications typically appear to be from a government agency or a legitimate business in order to trick you into divulging valuable personal information (including your birthday, Social Security number, passwords and PIN numbers) that can be used to commit identity theft. The emails and texts could also ask you to click on a link that will install malicious software on your mobile phone and enable the fraudster to gain access to your mobile banking apps.

Transaction alerts from your credit card, bank and mobile app provider… can help you identify unauthorized activity quickly.

"To protect yourself, never provide passwords, credit or debit card information, Social Security numbers and similar personal information in response to an unsolicited text message or email," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "If you have any questions regarding the legitimacy of an email or a text, call your bank or mobile app provider, or the business or government agency that claims to have sent the email or text, and be sure to use a phone number you have looked up on your own and not what is in the email or text in question."

Note: These messages are often called "phishing" emails and "smishing" text messages. Phishing is a term given to fraudulent emails "fishing" for valuable personal information, and "smishing" is a variation of that when referring to "Short Message Service" or "SMS" text messages. "Security experts for years have warned consumers about smishing scams, but as more people have smartphones, smishing is becoming more common," Benardo said.

Final Thoughts

When it comes to getting the most from mobile financial services, here's a simple strategy:

1. Review your bank's website to better understand the mobile products and services offered.

2. Read the bank's consumer disclosures to understand what assistance and other options may be available when using the institution's mobile technology.

3. Contact your bank directly with any questions or concerns, especially before you sign up for a new mobile banking or payment service.

Beware of ATM, Debit and Credit Card 'Skimming' Schemes

How to help protect yourself from high-tech thieves who steal account information

You may have heard in the news that automated teller machines (ATMs) are being targeted by criminals who secretly attach high-tech devices to the machines in order to record consumers' keystrokes and steal or, as it is sometimes called, "skim" personal identification numbers (PINs) along with credit or debit card account numbers. In addition, criminals are known to add similar devices to credit or debit card readers at checkout registers, especially at gas stations, convenience stores or other merchants where customers may be in a hurry and not notice or take the time to report something suspicious.

"Security experts and law enforcement officials warn that card skimming is present in many communities," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "With the information that can be skimmed, a thief can go on an online shopping spree or sell that valuable data to other con artists."

And how do thieves retrieve the data they gather? Some return to the scene of the crime to remove their devices, while others can communicate electronically with their hardware using a laptop or mobile phone and wireless connections.

Through the years, ***FDIC Consumer News*** has warned readers to be on the lookout for keystroke-recording devices on ATMs or checkout registers.

Here's a reminder of the different kinds of skimming devices and what to look for:

Card-reader overlays: The most common ATM skimmer, and perhaps the easiest device to detect, is the card-reader overlay. It is made of plastic and fits over the slot where you insert your card. As you insert your card, the device reads the data from your card and stores it. How can you tell if there's an overlay hiding an illegal card reader? "Before inserting your card, look at the card reader for signs it has been altered," said Amber Holmes, a financial crimes information specialist with the FDIC. "Be suspicious if your card doesn't easily go into the machine or if the card reader appears loose, crooked or damaged, or if you notice scratches, glue, adhesive tape or other possible signs of tampering."

Hidden cameras: While banks typically have security cameras near their ATMs to keep an eye on the area, thieves sometimes hide tiny cameras on or around ATMs. "If positioned correctly, a brochure holder on an ATM is the perfect place to hide a mini-camera that can record PIN numbers as customers type them," warned Benardo. "Also check for tiny holes in the ATM housing or in something else that looks like it was hastily stuck onto the ATM to cover a small camera."

PIN-capture overlays: Criminals have been known to attach dummy keypads over an ATM's real keypad to record and capture PIN numbers as they are entered. The keypad might be fake if it looks too thick or different from what you're used to seeing.

Fake ATM faceplates: Some thieves go as far as placing a fake ATM cover that could contain card-reader overlays, hidden cameras and PIN-capture overlays over some or all of a real, fully operating machine. "The best way to determine if an ATM has a false cover is to look for flaws like loose wires, seams that are not flush and slots or keypads that look out of place," said Holmes.

What should you do if you believe your debit or credit card account has been compromised?

There are consumer protection regulations that can help. For example, the Electronic Funds Transfer Act (EFTA) and the Consumer Financial Protection Bureau's (CFPB's) "Regulation E" limit a consumer's liability for losses from unauthorized transactions using his or her ATM or debit card or card numbers. If your debit card or the card number is used to make an unauthorized withdrawal from a checking or savings account, you can minimize your losses by contacting your bank as soon as possible. Your maximum liability under the EFTA is $50 if you notify your bank within two business days after learning of the loss. If you wait longer, you could lose more, according to the law. If it's your credit card number that is used without your authorization, your liability is normally capped by the Truth in Lending Act (TILA) and the CFPB's "Regulation Z" at $50 for all unauthorized transactions, and remaining credit card losses are typically absorbed by the card issuer.

"Even consumers who know the telltale signs of a skimming device may inadvertently use an ATM or a sales terminal that has been tampered with. That's why it's great to know that there are consumer protections available," said Tracie Greenway Morris, an FDIC senior community affairs specialist.

Some other worthwhile precautions you can take include:

- Do not use an ATM or a credit or debit card reader if anything looks suspicious, such as loose or extra parts. Alert the machine owner or the police immediately.
- Avoid ATMs in remote places, especially if the area is not well lit or not visible to security cameras and the general public. "ATMs in secluded locations are more likely to be altered," Benardo said.
- Go elsewhere if you see a sign directing you to only one of multiple ATMs in a location. It could be the machine that was tampered with by a crook.
- Shield the keypad with your hand when typing your PIN at the ATM or a retailer's checkout area. Doing so won't protect you from skimmers who use keypad overlays, but it will block the view of a hidden camera.
- Regularly check your bank and credit card accounts for unauthorized transactions, even small transactions that you think might not be worth reporting to your bank. "Thieves might make low-dollar withdrawals or charges as a way to test a counterfeit debit or credit card before they use it for big-dollar transactions," Holmes explained. "If you spot a potential problem, notify your bank as quickly as possible."

See additional tips in our Summer 2015 article on 10 ways to minimize fees and maximize security at the ATM (www.fdic.gov/consumers/consumer/news/cnsum15/atmtips.html). Also, the Federal Trade Commission has tips and information on what to do if your debit, credit or ATM card is lost or stolen at www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

Five Things to Know About Safe Deposit Boxes, Home Safes and Your Valuables

Over time, your valuables change, and so do your options to protect them. Here are a few choices, including safe deposit boxes and home safes, along with suggestions on how to assess each option for your specific needs.

1. Think about what should or should not be kept in a bank's safe deposit box. Good candidates for a safe deposit box include originals of key documents, such as birth certificates, property deeds, car titles and U.S. Savings Bonds that haven't been converted into electronic securities. Other possibilities for the box include family keepsakes, valuable collections, pictures or videos of your home's contents for insurance purposes, and irreplaceable photos.

Be mindful not to use your bank safe deposit box to store anything you might need to access quickly or when the bank is not open. That could include passports and originals of your "powers of attorney" that authorize others to transact business or make decisions about medical care on your behalf. For guidance on where to store your original will, check with an attorney about what is required or recommended based on state law.

2. You're better off stashing your cash in a bank deposit account, like a savings account or certificate of deposit, than in a home safe or a safe deposit box. Among the reasons: "Cash that's not in a deposit account isn't protected by FDIC insurance," noted Luke W. Reynolds, Chief of the FDIC's Community Outreach Section. That's because, by law, the FDIC only insures deposits in deposit accounts at insured institutions and only in the rare instances when a bank fails. A safe deposit box is not a deposit account. It is storage space provided by the bank, so the contents, including cash, checks or other valuables, are not insured by FDIC deposit insurance if damaged or stolen. Also, financial institutions generally do not insure the contents of safe deposit boxes. If you want protection for the valuables in your safe deposit box or home safe, talk to your homeowner's or renter's insurance agent about adding coverage under these policies.

"And unlike money in a savings account, money in a home safe or safe deposit box cannot earn interest, so the purchasing power of your cash will decrease," said Reynolds.

Also read the terms of the safe deposit box rental agreement, as the bank may limit what you can keep in the box. These limitations could include cash.

3. A home safe isn't a true replacement for a bank's safe deposit box. A home safe could be used to store replaceable items you may need immediate access to, such as a passport. But home safes are not as secure as safe deposit boxes. "A burglar could more easily break into your home and open the safe than get inside your safe deposit box at your bank," said Reynolds.

4. No safe deposit box or home safe is completely protected from theft, fire, flood or other loss or damage. Consider taking precautions, such as protecting against water damage by placing items in water-safe, zippered plastic bags or other plastic containers that can be resealed. And, don't keep identifying information on or near your safe deposit box key, such as the box number and the bank's name, in case of loss or theft. Remember that, by law, FDIC insurance covers only deposit accounts. Also, don't expect the bank to reimburse you for theft of or damage to the contents of your safe deposit box. Again, you can ask your insurance agent about providing some coverage in your homeowner's or renter's policy.

5. Be careful who you allow to access your safe deposit box. You can jointly rent a safe deposit box with one or more people who you would like to give unrestricted access. Keep in mind, though, that your bank would likely not be responsible for anything that people you authorize to enter the box remove without your permission.

Who has access to your safe deposit box if you die? "The rules under which

safe deposit boxes may be accessed upon the death of a safe deposit box owner depends on state law," said FDIC Counsel Richard Schwartz. "These rules restrict entry into the safe deposit box to certain individuals and permit entry only under controlled situations."

For additional tips on keeping financial papers and valuables secure and accessible, see the article in our Summer 2014 issue at www.fdic.gov/consumers/consumer/news/cnsum14/whattokeepwhere.html.

This is an updated version of an article originally published in the Fall 2009 ***FDIC Consumer News.***

The FDIC and National Consumer Protection Week 2018

The FDIC celebrates National Consumer Protection Week (NCPW), March 4-10, 2018. This nationwide campaign was created to help individuals make better-informed financial decisions. Please visit our question-and-answer pages, which will be updated each weekday of NCPW, plus additional consumer tips and information for reference year-round at www.fdic.gov/ncpw.

New Standards for Credit Report Accuracy May Help Consumers

The three major consumer credit reporting companies — Experian, Equifax and TransUnion — have new standards to enhance the quality of the credit reports they produce. The changes are in response to a 2015 legal settlement requiring action by these companies to reduce errors on credit reports. Incorrect or outdated negative information on a credit report can adversely affect a consumer's ability to borrow money under the most favorable terms, so it is important to make sure the information is correct.

When consumers apply for a loan or a credit card, the lender's approval and interest rate provided are determined in part by information contained in credit reports, as well as credit scores. Credit reports summarize an individual's credit history — for example, how many credit accounts were opened in recent years and whether bills are paid on time. Credit scores are developed by scoring companies, such as FICO (the Fair Isaac Corporation), based on repayment history and other information included in credit reports. The higher a person's credit scores, the more likely he or she is to qualify for credit, rental housing, insurance and, in certain circumstances, employment. That's why it is important that the information in a credit report is complete and accurate.

In response to the settlement in July 2017, Experian, Equifax and TransUnion began removing tax liens (a legal claim on the assets of a delinquent taxpayer) and civil judgment debts (court-ordered payment of damages) from consumer credit reports, if the information is incomplete.

Experian, Equifax and TransUnion also agreed to exclude medical debts on consumer credit reports until such debts are at least 180 days past due. According to a 2014 report by the Consumer Financial Protection Bureau (CFPB), medical debt has been a source of numerous complaints because the billing process can be complicated and confusing. As of September 15, 2017, the new 180-day waiting period gives consumers time to resolve medical billing issues.

What You Can Do

"While the changes in reporting standards can mean that some negative information will be removed from peoples' credit reports, which is beneficial, consumers still need to understand what is on their credit reports and take steps to ensure that they are accurate," said Elizabeth Ortiz, the FDIC's deputy director for consumer and community affairs.

Examples of credit reporting errors may include outdated information, missing loan payments, incorrect Social Security numbers, or reporting on individuals with similar names or addresses.

What are some simple precautions you can take to build your credit history and preserve good credit scores? In particular, review your credit reports at least once a year to look for discrepancies and errors. "Make sure you're familiar with the information in your credit reports before you apply for a new job or a loan," said Kristin Strong, chief of the FDIC's Consumer Response Center. "Correcting any errors in advance could help you qualify for a better interest rate on a loan and save you from being denied access to credit, employment, housing or even insurance."

It's also important to note that because there are multiple credit scoring models, credit scores may vary. As explained by Heather St. Germain, an FDIC senior consumer affairs specialist: "You can't control which score a lender uses, but you can help produce good scores by having a positive credit history and checking your credit reports often to correct mistakes."

> ***"Consumers need to understand what is on their credit reports and take steps to ensure that they are accurate," said Elizabeth Ortiz, the FDIC's deputy director for consumer and community affairs.***

The Fair Credit Reporting Act requires each of the three nationwide credit reporting companies to provide you with a free copy of your credit report once every 12 months, only upon request. To obtain your free credit reports, go to www.annualcreditreport.com or call toll-free 1-877-322-8228. Note, that unlike credit reports, you may be charged a fee to obtain your credit scores.

Another important reason to check your credit report is to look for possible signs of identity theft or fraud. Warning signs include an unfamiliar credit card or loan listed in your name. The sooner a fraudulent account is identified in your credit report, the sooner you may be able to limit financial harm.

Inaccurate credit report information can be disputed directly with the applicable creditor or online with each of the three major credit reporting agencies: Equifax at www.equifax.com, Experian at www.experian.com and TransUnion at www.transunion.com.

For additional information on credit reports, visit the FDIC's webpage at www.fdic.gov/consumers/assistance/protection/creditreport.html. To learn more about how to improve your credit scores, see the Summer 2015 ***FDIC Consumer News*** (www.fdic.gov/consumers/consumer/news/cnsum15/creditscores.html).

The Home Mortgage Appraisal: How Consumers Can Benefit

A home appraisal is often required as an essential component of the mortgage financing process. Because the consumer pays the cost of the appraisal when applying for a mortgage to buy or refinance a home, it's worth learning more about what the consumer is getting for the money, and why lenders typically are required to obtain an appraisal or another type of property valuation. "What many people may not know is that an appraisal is one of the most important parts of the home mortgage process because it can help the buyer as well as the lender," said Elizabeth Ortiz, the FDIC's deputy director for consumer and community affairs.

First, the basics. The appraiser must provide an independent estimate of the "fair market" value of the property in comparison to similar homes in the area. This is one method the lender uses to avoid making a loan that is too large in relationship to the property's appraised value, commonly referred to as the "loan-to-value" or LTV ratio. According to Sandra Barker, a senior policy analyst at the FDIC, "The appraisal helps ensure that the loan can be paid off if the borrower doesn't make all the payments as agreed and the property needs to be sold at a later date."

The appraised value can play a role in the interest rate applicants are offered, too. If the appraised value of the home comes in significantly higher than the loan request, the lender may have guidelines that make it possible to offer a more favorable rate.

Appraisal rules require lenders to send applicants a copy of the full appraisal report or other written valuation "promptly" after receiving it but at least three days before the loan closes. What's good to know is that the information in an appraisal report may sometimes assist buyers in negotiating a lower price from the seller.

Here are the key things to look for in the appraisal report:

- Does the report show the correct number of bedrooms and baths, and contain references to a garage, a pool and so on?
- Is the square footage in the report relatively similar to what is in official records?
- Are the comparable home sales used to determine the value of the property located close to the house being purchased? Also, did those houses sell within the last six months?
- Is there something else the appraiser left out that might contribute to the home's value? For example, were all significant "improvements" to the home listed in the appraisal report and accounted for in the final value?

"If borrowers have concerns about their lender's appraisal report, they can provide additional information to the lender that could prompt the appraiser to reevaluate its determination of the home's value," said Susan Welsh, a senior consumer affairs specialist at the FDIC. "Some consumers decide to pay for another appraisal by a different company. While that second appraisal can't be accepted by the lender as proof of value, it may provide additional information that can be used to challenge the lender's appraisal."

For questions regarding home appraisals, a good place to start is with FHA Resource Center (call 1-800-225-5342 or send an email to answers@hud.gov). To register a complaint about an appraiser or a lender, you can start by contacting the Appraisal Subcommittee of the Federal Financial Institutions Examination Council for a reference to the appropriate authorities (call 1- 877-739-0096 or go to https://refermyappraisalcomplaint.asc.gov/default.aspx).

FDIC
Consumer News

Published by the Federal Deposit Insurance Corporation

Martin J. Gruenberg, *Chairman*

David Barr, *Assistant Director, Office of Communications (OCOM)*

Jay Rosenstein, *Senior Writer-Editor, OCOM*

Aileen Wu, *Graphic Designer*

FDIC Consumer News is produced quarterly by the FDIC Office of Communications in cooperation with other Divisions and Offices. It is intended to present information in a nontechnical way and is not intended to be a legal interpretation of FDIC or other government regulations and policies. Due to periodic changes in statutes and agency rules, always check the FDIC Web site — www.fdic.gov — for up-to-date information. Mention of a product, service or company does not constitute an endorsement. This publication may be reprinted in whole or in part. Please credit ***FDIC Consumer News***.

Send your story ideas, comments, and other suggestions or questions to: Jay Rosenstein, Editor, ***FDIC Consumer News,*** 550 17th Street, NW, Washington, DC 20429, e-mail jrosenstein@fdic.gov.

Find current and past issues at www.fdic.gov/consumernews or request paper copies by contacting the FDIC Public Information Center. Call toll-free 1-877-ASK-FDIC (1-877-275-3342) or e-mail publicinfo@fdic.gov.

Subscriptions: To receive an e-mail notice about each new issue with links to stories, go to www.fdic.gov/about/subscriptions/index.html. To receive ***FDIC Consumer News*** in the mail, free of charge, call or write the FDIC Public Information Center as listed above.

For More Help or Information

Go to www.fdic.gov or call the FDIC toll-free at 1-877-ASK-FDIC (1-877-275-3342)

A Final Exam: Test Your Money Management IQ

A quiz based on tips and information in this issue

1 As a security precaution if the mobile phone with your banking app is lost or stolen, experts recommend setting the screen on the phone to lock after a certain amount of time. **True or False?**

2 The terms "phishing" and "smishing" refer to fraudulent emails and text messages, respectively, that are intended to trick consumers into divulging information such as usernames and passwords that can enable identity thieves to access bank accounts. **True or False?**

3 The term "skimming" refers to when criminals attach high-tech recording devices and tiny cameras on or around automated teller machines (ATMs) and store checkout registers in order to steal consumers' credit or debit card account numbers and personal identification numbers (PINs). **True or False?**

4 Money that you put into your safe deposit box at a bank is insured by the FDIC. **True or False?**

5 Your "credit report" and your "credit score" are two names for the same thing. **True or False?**

6 Recent changes have given consumers more time to resolve billing issues with medical providers and insurers before the debt owed appears as negative information in their credit reports. **True or False?**

7 If you apply for a mortgage loan to buy or refinance a home you are generally required by the lender to pay for an appraisal, which is an independent estimate of the "fair market" value of the property. **True or False?**

Correct Answers

1. True (See Page 3)
2. True (See Page 3)
3. True (See Page 4)
4. False (See Page 5)
5. False (See Page 6)
6. True (See Page 6)
7. True (See Page 7)