In this unit, you will:

- Become familiar with the various types of financial services providers
- Examine how a savings account works
- Practice using a checking account and debit card
- Explain how a credit card is used to make purchases
- Explore the features of automated financial services
- Respond to situations involving identify theft and deceptive practices

UNIT FIVE

Your Money: Keeping It Safe and Secure

Once you've started earning money, you have to figure out the best way to spend it. Not what to spend it on necessarily—you already did that with your spending plan in Unit 2. But *how* you're going to spend it—how you're going to actually pay bills and make purchases, including those big ones you've saved for.

We have more options than ever before when it comes to financial services—different types of accounts and financial institutions and different ways of moving money around. They all come with their pros and cons, and choosing the right one for you can seem overwhelming.

So this unit covers all the bases of financial services. You'll learn about savings and checking accounts and debit and credit cards. We'll also look at how automated services can make your life easier and consider hazards to look out for, such as identity theft.

What Do You Think?

1. More than ____% of teens have a savings account.
2. ____% of teens ages 16–17 have a checking account. ____% of those ages 18–19 have one.
3. Likewise, only ____% of teens ages 16–17 have a debit card. ____% of those ages 18–19 have one.
4. Among teens ages 16–17, ____% have one of their parents' credit cards.
5. ____% of teens ages 16–19 have their own credit card.

Source: Teen Research Unlimited 2005

Who's Who in Financial Services

When it comes to taking care of your basic financial needs, the first step is finding a bank or credit union. A ***bank*** is a for-profit company, owned by investors in its stock. These stockholders elect a paid board of directors to manage the bank for them. Anyone can walk up to a bank and open an account.

Credit unions are financial institutions owned by their customers, who are also called members. These members elect a volunteer board of directors (who are also members) to manage the credit union for them. But credit unions have membership qualifications. By law, each credit union must serve a defined segment of the population. To join a credit union, you have to work for or have a family member who works for an employer in that segment.

Aside from an employer-sponsored credit union, you may be able to join another type of credit union by becoming a member in a church or social group, by having a certain type of job (say, a school teacher), or by living or working in a certain community.

Despite their differences, both banks and credit unions can meet your needs. Both provide a variety of basic financial services, including savings and checking accounts, issuing credit and debit cards, and providing loans for cars, homes, and other purposes.

Exercise 5A:
What Do They Offer?

Visit the Web sites of at least two financial services providers. List the services provided and be prepared to share what you have learned.

Assignment 5-1:

Shopping for My Financial Services Provider

Use the decision-making process to select a financial services provider for your personal use. Be sure to consider your criteria as you compare the services of at least three providers.

A ***savings account*** (at a bank) or ***share account*** (at a credit union) is a place to deposit money you don't plan to spend right away. You'll remember that we discussed savings accounts in Unit 3. When it comes to setting aside money for your financial goals, you can get cash out of a savings account quickly and without penalty. This makes a savings account a good place for short- to medium-term financial goals. Finally, some banks and credit unions make it easy to save by allowing you to set up an automatic savings plan, where money is automatically transferred from your checking to your savings account every month.

Fees for savings accounts are usually pretty minimal, but be sure to read the fine print before you open an account. And check out ***Figure 5-1*** for more information on what fees to watch for.

Opening a savings account is a cinch. Take cash or a check made out to the financial institution of your choice for your first deposit. You'll also need to bring picture identification, such as a driver's license, passport, or student ID. Check with the financial institution to find out what and how many forms of ID it requires. Make sure you also take your Social Security number. You will be asked to fill out a few forms with your address and phone number, date of birth, and maybe some current employment information. You will also have to sign what's called a signature card to verify that a signature is yours later if necessary.

Once you make your first deposit, you'll receive monthly statements showing your account balance. This is simply a total of your deposits, withdrawals, and interest earned. And when you're ready to spend money in your savings account, you can fill out a withdrawal slip and get cash, fill out a transfer slip and move money to your checking account, or possibly withdraw your money through an ***automated teller machine (ATM).***

Your biggest responsibility with a savings account is to keep your account number and information in a safe place. You also need to review your monthly statement and make sure all of the deposits and withdrawals listed on your statement are correct and that there are no unauthorized withdrawals or errors. It's rare, but mistakes do happen.

Banks and credit unions are responsible for keeping your money safe and giving it to you, with interest, whenever you ask. Your bank also agrees to continue to carry government insurance to protect up to $100,000 of your deposits.

Exercise 5B:
Read the Fine Print

Read a sample agreement for a savings account. What are the features of the account? What are the conditions of using the account?

Exercise 5C:
Make the Deposit

Imagine that you received $100 in cash for your birthday and decide to deposit the money in a savings account for one of your goals. Use the form below to fill out a savings deposit slip. Use 101-23456-678 for the account number.

DEPOSIT

CHECKING ☐
SAVINGS ☐

Today's Date

Customer Name

Customer Address, City, State, Zip

Sign Here (If cash is received from this deposit)

X

CASH

CHECK

TOTAL FROM OTHER SIDE

SUBTOTAL

LESS CASH

ACCOUNT NUMBER

TOTAL $

Check in With Checking Accounts

There are many reasons to open a ***checking account,*** called ***share draft accounts*** at credit unions. Maybe you don't feel safe walking around with a lot of cash and want a safe place that offers easy access to your money. Or maybe you just know that cash in your pocket is too easily spent! Whatever the reason, many people like to use a checking account to manage their day-to-day finances.

Like a savings account, you simply take cash or a check made out to the bank to open an account and make your first deposit. And remember to take your Social Security number and two or more forms of picture identification. Again, you'll have to fill out a few forms with some basic information. Once you open the account, you'll receive a box of checks in the mail, preprinted with your name and address, along with a check register to record your transactions. You'll also begin getting monthly statements.

Writing a check is like creating a mini-contract between you and the person or business you're paying. When you sign at the bottom of the check, you're agreeing to pay the person, named on the "Pay to the Order of" line, the amount you specified, on demand. On demand means that your bank must honor your check by paying the specified amount to the payee (the person or business to whom you wrote the check) when she or he cashes it as long you have enough money in your account to cover it. Get into the habit of recording each check you write into your checkbook register, along with your deposits and withdrawals. And always write all checks in ink.

When you receive a check, the process works in reverse. You take the check to your bank or credit union, and sign (or ***endorse***) it on the back. Your bank or credit union will cash the check or credit your account for that amount, and the funds will be transferred from the payer's bank or credit union over to yours. Sometimes, if the check is for a large amount or from an out-of-state bank, your deposit may be held a few days before you can have access to your money. In this way, the bank has time to verify that the payer actually has enough money to cover the check.

There are many benefits to using a checking account:

Convenience. If you use checks, you don't always have to have cash before making a purchase. And you shouldn't send cash through the mail, just checks, to pay bills. Also, you can usually access your checking account by using your debit card at an ATM.

Safety. You don't have to carry a big wad of cash when you go shopping. Also, stolen checks can be replaced. Lost or stolen cash cannot—it is, simply, gone.

Easier Budgeting. A checking account can also help you budget your money. When you use your check register to record whom you wrote checks to, you're automatically keeping track of where your money is going—making it easier to evaluate your spending habits.

Proof of Payment. Checks provide written proof that you made a payment to someone or a business. Each time you write a check that ultimately clears your account (when the money is taken from your account and added to the payee's account), there will be several records of it—making it easier to prove that you did in fact make a payment, should anyone ever challenge you about it.

The catch is you usually pay for these benefits in the form of fees automatically deducted from your account. While you may see ads for "free" checking accounts, you should know that no checking account is completely free. Even if there is no monthly fee, you *could* end up paying some of the fees described in ***Figure 5-1.***

Follow the Bouncing Check

David wrote a check for $65 to a clothing store, figuring he would cover the purchase by depositing his paycheck the next day. But when the store deposited David's check into its account, instead of receiving payment from David's bank, his check "bounced" back to the clothing store due to insufficient funds in his account. The store then sent David a notice stating that he still needs to pay the $65, plus another $25 for writing a bad check. Additionally, David's bank deducted an insufficient funds fee of $30 from his account, drawing it down to only $20.

But David was on a spending spree. He wrote another check to an auto parts store that same day for $25. So that check bounced, and the auto parts store sent him a notice stating that he still needs to pay the $25, plus another $25 for writing a bad check. And David's bank deducted another insufficient funds fee of $30 from his account, drawing it down to –$10.

Prior to all this happening, had David written any check that had not yet cleared, it too would bounce, and he'd rack up more rounds of bad check and insufficient funds fees.

But even if nothing else happens, David will have written two bad checks totaling $90, paid $110 in penalties, for a total cash outlay of $200!

Of course, you're responsible for making sure your account information and checks are stored in a safe place. And while everyone makes an occasional mistake, it is your responsibility to keep track of your balance and make sure you have enough money in your account when you write a check.

The consequences of misusing a checking account can be far greater than just paying fees. If the bank decides you have an excessive number of overdrafts, it may close your checking account. This could be reported to the credit bureaus. A history of checking account abuse can prevent you from obtaining another checking account and damage your credit history. And intentionally writing checks without enough funds to cover them is considered check fraud—a serious crime.

Some other things to consider when you open an account at a bank or credit union include:

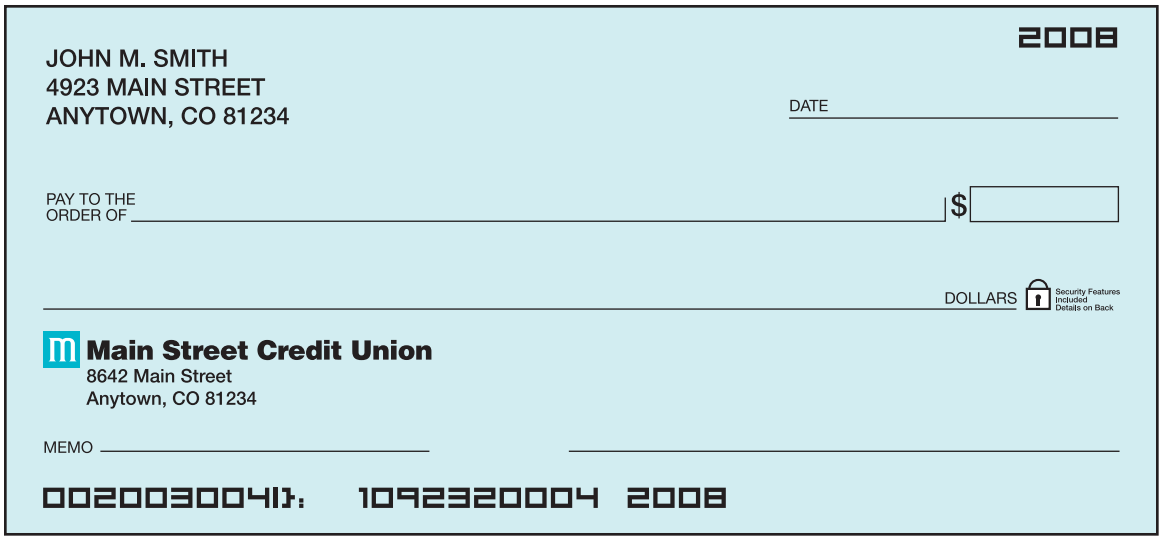
- Is it convenient for you? Will you be able to get there during the hours it's open if need be? Does it have ATM locations in neighborhoods you frequent? Does it let you use other banks' ATMs free of charge, several times a month?
- Does it offer other services you're interested in, such as online banking?
- Do you meet the institution's age requirement for a checking account? If not, you'll need an adult co-signer to open an account.

Along with these account responsibilities come your rights. You can get your money whenever you ask. Your deposits are insured for up to $100,000. And, you can expect to be apprised of any changes in fees or terms of your account.

If you find a mistake when you check your monthly statement—say, a withdrawal you didn't make, a duplicate purchase, or an incorrect deposit amount—you have the right to ask your bank to investigate the error. And if the bank finds an error, you have the right to have your account corrected.

It is definitely safer to carry checks than cash, but of course, you still have to be careful. People who find blank checks you've lost can try to alter them or forge your signature. So it's smart to take a few precautions:

1. Always write checks in ink.
2. Once you endorse a check (sign the back of it), anyone can cash it. So don't endorse checks you plan on depositing until you get to the bank or credit union. As an added measure of security, some people like to write "For Deposit Only" and their account number underneath their endorsement.
3. Keep unused checks in a safe place.
4. Check your statement every month to make sure there are no withdrawals you didn't authorize and that your activity matches what you recorded in your checkbook register.



Exercise 5D:

Keeping Track

Record the following transactions in the checkbook register. Is your final balance $201.65?

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Opened checking account with cash deposit, $200 Automatic withdrawal to pay for personalized checks, $20		Wrote Check #100 at Fine Foods to buy groceries, $23.11 Wrote Check #101 to buy books at Wayne's Book World, $13.50	Wrote Check #102 to self for "Cash" to have spending money for the weekend, $30	Automatic withdrawal for monthly phone bill, $25.50	Deposited paycheck, $113.76

NUMBER OR CODE	DATE	TRANSACTION DESCRIPTION	PAYMENT AMOUNT	✓	FEE	DEPOSIT AMOUNT	$ BALANCE
			$			$	

Exercise 5E:

Does It Balance?

Reconcile Ryan's checking account to ensure that his records match his credit union's records. Use the checking account information and statement provided by your instructor to complete this exercise.

The DNA of Debit Cards

Debit cards, sometimes called "check cards," have credit card logos on them but are very different. Instead of drawing on a line of credit, debit cards act like a check, deducting the amount of your purchase from your checking account. The good news is there's usually no interest associated with your debit card purchases because you're not actually borrowing money (you're drawing down your checking account instead).

When you flip over a debit card, the first thing you'll probably notice is the black magnetic strip. That's basically the intelligence center of the card. It stores data such as your name, account number, ***personal identification number (PIN),*** and financial limits. So you should be careful to protect it! If you accidentally wash the card, place it too close to a magnet, or scratch the strip, your card may not work anymore.

When you're at a store buying something with a debit card, you usually have to choose one of two options: to use it as a credit card—including having to sign for your purchase—or to use it as a debit card. In both cases, you or the cashier will have to swipe your card through an electronic terminal. But if you choose to use it as a debit card, you'll be prompted to enter your PIN. (And you may be asked if you want to get cash back, a handy way of making a withdrawal along with your purchase.) The terminal will then indicate whether the transaction was approved. If it was not, you must find another way to pay for your items.

Debit cards offer many of the conveniences of a credit card. They're particularly useful to people who don't like to carry a lot of cash and don't want to be tempted into accumulating too much debt. Compared with checks, there's less to carry, and checkout transactions usually go faster. But if you're not diligent about recording your debit card purchases and withdrawals in your checkbook register, you can end up with too little money to pay bills or a bounced check. And of course, someone who steals your debit card can use it to wipe out your account before you even know it's gone.

So how do you get a debit card? You will usually be asked if you want one when you open your checking or savings account. But you'll have to wait until you receive the card in the mail before you can actually use it. For security purposes, you'll receive your PIN in a separate letter.

Once you get your debit card, you can use it at one of your bank's or credit union's ATMs to make deposits into your account, or you can use it at almost any ATM to withdraw money. Simply swipe the card, enter your PIN, and follow the instructions on the ATM screen.

But remember—accurate record keeping is key. So whether you use the card to deposit, withdraw, or make purchases, make sure you record what the transaction was and how much it was for.

There's usually no additional charge to get a debit card for your account. But there may be charges for using it. Always read the terms of the debit card agreement carefully to find out what kinds of charges you might be assessed and for how much. Some of the fees you may encounter are outlined in ***Figure 5-1.*** However, fees vary widely, so it pays to do your homework to find out the least expensive ways to use your debit card.

Your rights and responsibilities with a debit card are virtually identical to those of a checking account, with the added responsibility of immediately reporting a lost or stolen debit card. Even without your PIN, someone can steal and use your debit card as if it were a stack of blank checks. As you can imagine, this wreaks havoc on your checking account if you don't notice the theft right away—wiping out all the money you've earned to pay for bills and life's little necessities.

Unfortunately, you have less protection against fraud with a debit card than with a credit card. If you report a missing card within two business days after you realize that it's missing, you'll only be responsible for up to $50 of unauthorized charges. Wait longer than that, though, and you could lose up to $500. And if you see an unauthorized transaction on your monthly statement and wait more than 60 days to report it, you could be liable for the entire amount.

In short, if you do lose your debit card or find unauthorized uses on your monthly statement, it is critical to report them to the card issuer right away.

7 Signs of Smart Debit Card Use

1. Memorizing and protecting your PIN (don't choose something obvious like your house address, phone number, or birthday) and not carrying it in your purse, wallet, or pocket. **Remember, theft of your PIN can wipe out your account and leave you with overdraft fees.**
2. Immediately recording purchases and withdrawals in your check register.
3. Signing the back of your card to make it harder for others to use.
4. Keeping receipts to check against your statement.
5. Using your institution's ATM machines to avoid fees.
6. Being aware of your surroundings when you use your debit card, especially at an ATM at night.
7. Immediately reporting lost or stolen cards.

Figure 5-1: Fast Facts About Financial Services Fees

Types of Fees	Accounts They Affect	When They May Be Charged
Monthly service fees	Savings and checking accounts	If you don't meet certain qualifications, such as maintaining a monthly minimum balance or limiting the amount of checks you write
Withdrawal fees	Savings accounts	If you exceed a certain number of monthly withdrawals
ATM or debit fees	Savings and checking accounts accessed by a debit card	By your bank when you use an ATM machine. May be waived if you use your financial institution's own machines
Third-party ATM fees	Savings and checking accounts	If you use another bank's ATM, a charge assessed by that bank
Returned check fees	Savings accounts	If a check deposited into your account is returned for insufficient funds
Check fees	Checking accounts	When you purchase your own checks preprinted with your name and address
Insufficient funds or overdraft fees	Checking accounts	When you write a check but don't have enough money in your account to cover it
Stop payment fees	Checking accounts	When you ask your financial institution to stop a check drawn on your account from being cashed
Point-of-sale fees	Debit card accounts	When you use your debit card as a debit card at a store or gas station
Over-the-limit fees	Credit cards	If you go over your spending limit
Annual fees	Credit cards	Charged by some credit card companies for the yearly use of their credit cards

Assignment 5-2:

Use a Checking Account

Practice recording two months of checking account transactions. At the end of each month, reconcile your balance with the monthly statement balance. Use the checking account information provided by your instructor to complete this assignment.

Credit Card Confidential

While debit cards give you access to your own money, a credit card is a separate supply of money. When you use a credit card, you are simply taking a loan from the company that issued the card (the "issuer"). Your purchases are then totaled and sent to you in a monthly bill or statement. In most cases, if you pay your bill in full and on time, you'll owe no interest. Visa®, MasterCard®, and Discover® are all examples of major credit cards.

We talked in Unit 4 about places to look when you're ready to get your first credit card. Your current bank or credit union and retail stores are usually your best bet. Or instead, you could ask a parent to co-sign on your first card. Whatever route you choose, you'll have to provide basic information about yourself on the application, including your employer and annual income. Some stores will phone in your application and make a credit decision on the spot. With banks and credit unions, you may have to wait a couple days to find out whether or not your application is approved.

Every credit card has a credit limit—the maximum amount that you can have charged on the card at any one time. Be sure to sign the back of your card before you put it in your wallet. This will help stores verify your signature.

If the card allows you to withdraw cash, you will also receive a PIN in the mail. But unlike a debit card, you'll pay interest immediately on credit-card cash withdrawals. In fact, sometimes you'll pay a higher rate of interest for cash withdrawals charged to your credit card than for purchases. So that's another reason to read carefully the terms and conditions that arrive along with your new card.

When you make a purchase, you or the cashier will swipe your card through an electronic terminal. The charge will be added to your account, reducing the available credit limit left on your card, and you'll receive a receipt for your purchase. You should save your receipt until you reconcile it with your monthly statement.

Your purchases are totaled on a monthly bill or statement. If you have a balance from the previous month, your monthly bill will display a finance charge added to your balance. Any payment you make is then deducted from your total balance. And that balance, subtracted from your credit limit, indicates what your available credit is (the amount you can still spend on the card without going over your limit).

Always avoid going over your credit limit, and try to pay off the entire balance each month to avoid interest and fees. Unlike your debit card, your credit card issuer won't necessarily deny a charge that will put you over your credit limit. It may just accept it and then hit you with an over-the-limit fee.

Each time you receive a bill, check to make sure that your previous month's payment has been credited to your account. It's also important to review all listed charges for accuracy. If you've been saving your receipts, it'll be easier to remember your purchases and to clear up any confusion if the business name on your credit card bill isn't familiar to you. It'll also help you discover any errors or unauthorized charges. If you do find an unauthorized charge, contact your credit card company immediately.

Exercise 5F:
What Would You Do?

What would you do if your credit card was stolen? Are you responsible for any unauthorized purchases? Read the terms of a credit card to learn what to do if your card is stolen.

As with other financial services, you agree to certain responsibilities and rights as an account holder. The same holds true for your credit card account. You agree not to let anyone else use your credit card. You promise to repay the entire amount you charge, with interest, and to make at least a minimum payment on time each month. And you agree to notify the issuer promptly if the card is lost or stolen, or if you suspect that it's being used without your permission.

Of course, you have rights as well. You have the right to know how the finance charges on your account are calculated. If you contact the company about a possible error on your account, you have the right to get your account corrected or receive an explanation within 90 days. If you have a problem with the quality of products or services you bought with the card, you may have the right of not paying the remaining amount due.

Say you're looking at your bill one month and see a couple of charges you don't recognize from someplace in Brazil. You know you've never bought anything from Brazil, much less been there. What do you do?

First, look for the customer service phone number on your credit card statement. Call it and tell the representative that your bill has several charges that you don't recognize, and identify which ones they are. The credit card company should open an investigation by contacting the business that posted the charges to your account and getting more information about who made the charges to your account. In the meantime, your credit card company should remove the questionable charges from your bill so you don't have to pay interest on them.

In about 30 to 60 days, you'll receive a letter letting you know the results of the investigation. If the credit card company finds out that the charges were due to an error or to fraud, it won't do anything further (because it already took them off your bill). But if it finds out that you did in fact make the charges, the credit card company will add them back to your bill, plus interest.

Of course, if your credit card is ever lost or stolen, you should not wait for your monthly bill to arrive before you report it. Find the customer service phone number on a previous bill or the company's Web site and call it immediately. A company representative will look to see if anyone has used your card since you noticed it missing, then cancel your account. In about a week or so, you'll get a new card with a new account number in the mail. But in the meantime, no one can use your current account. By law, your liability is limited to $50 if your credit card is lost or stolen—so the credit card company can't make you pay any more of the fraudulent charges than that if you report the theft promptly.

Assignment 5-3:

Choosing a Credit Card

Compare at least three credit cards, and choose the one that has the best deal.

Automating Access to Your Money

Like everything else, the Internet has revolutionized financial services. ATM machines provide 24–7 access to cash anywhere in the world. Depending on the machine's services, you might also be able to check your account balance, make deposits, transfer money between checking and savings accounts, and even buy postage stamps.

Online banking means you can view your savings and checking account activity, transfer money between accounts, and even pay bills with just a few clicks of the mouse. Once you have access to your account online, you can log on and do your financial business from any Internet-enabled computer in the world.

EFT stands for ***electronic funds transfer.*** It allows employers to deposit your paycheck directly into your account instead of giving you an old-fashioned paper check that you need to deposit in person. It connects your drugstore purchase made with a debit card to your bank or credit union, then transfers money from your institution to the drugstore's account. It's also behind making transfers to your creditors when you make online bill payments from your checking account. And sometimes when you pay a business with a check, it uses EFT to do what's known as electronic check conversion. This converts a paper check into an electronic payment and immediately deducts the amount of the purchase from your account. So be sure to keep enough money in your account to cover any EFT payments so they don't bounce.

Exercise 5G:
The Pros and Cons of Automated Services

What do you think the benefits of automated services are? What do you think are the concerns of using automated services?

In short, automated services offer:

Convenience. You can access your money virtually anytime, anywhere.
Personal Safety. You don't ever have to carry a lot of cash with you.
Knowledge. You can track exactly how much is in your account on a daily basis.
Time Savings. You can make more time for fun using direct deposits and paying bills online.

Don't forget that automated services may come with fees, and there is no common practice. So again, it really pays to do your research before choosing a financial services institution. And comparison shop from time to time afterward to make sure you're still getting a good deal.

And of course, security is an issue. You're responsible for keeping your personal information safe. Credit unions and banks know that customers expect their transactions to be secure, so they take great care to ensure that conducting financial business with them is secure no matter where you do it. But security issues do arise, and the chances of your information being stolen increase when you use these automated services.

Assignment 5-4:

What Are the Trends?

What's happening in the world of online financial services? Select an online financial service that is of interest to you. Learn about the features of the service, and share what you have learned.

So Many Choices ...

Different types of accounts, a variety of features, big differences in fees—all the factors in choosing financial services can be overwhelming. So let's revisit the decision-making process again.

1. **Set goals.** What do you plan to use the account for? What features would be most useful to you?
2. **Establish criteria.** What financial products and services do you want and need?
3. **Explore your options.** Which type of account is best suited to your goals? Compare the services of several providers on requirements, features, fees, and convenience.
4. **Weigh the pros and cons of the options.** Decide which financial services provider offers the best services for your goals.
5. **Make a decision.** Apply to open the account. Set up new files to stash the terms and conditions and, later, your monthly statements.
6. **Evaluate your decision.** Are you getting what you expected out of the account? Has the provider changed any of the terms? If it has been a while since you chose a provider, are there any better deals now?

Using financial services software along with online account services such as online banking can be the next step in automating your financial record keeping. Software can make it easier to track your finances and create and adjust your spending plan. When you enter checks and deposits into the software as they occur, it can practically reconcile your account for you. Many financial institutions allow you to download checking and credit card statements directly into the software to minimize data entry. There are many personal finance software programs.

When Fraud Comes Knocking

Identity theft occurs when someone uses your name, Social Security number, credit card number, or other personal information without your permission. It is a very serious crime. People whose identities have been stolen can spend months or years—and thousands of dollars—cleaning up the mess thieves leave behind. In the meantime, victims of identity theft may lose job opportunities, be turned down for loans, and even get arrested for crimes they didn't commit.

Whether your personal information is accidentally disclosed or deliberately stolen, it can result in big trouble for you if it ends up being used for identity theft. Some of the many ways identity thieves can create problems for you are:

- Opening new credit card accounts in your name. When thieves use the credit cards and don't pay the bills, the delinquent accounts show up on your credit report.
- Opening a new account in your name and writing bad checks on the account.
- Forging your signature on blank checks or authorizing electronic transfers in your name, draining all the money from your accounts.
- Filing for bankruptcy under your name to avoid paying debts they've incurred under your name or to avoid eviction.
- Buying a car by taking out an auto loan in your name.
- Getting identification, such as a driver's license, issued in your name but with their picture.
- Giving your name to the police during an arrest. If the impostor doesn't show up for the court date, an arrest warrant is issued in your name.
- Changing the billing address on your credit card account (or by completing a "change of address" form at the post office), then running up charges on it. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.

Unfortunately, identity theft has become big business all around the world. Sometimes you have no control over your personal information falling into thieves' hands. If an employee steals your records or a hacker breaks into a business or government agency's database, you could be in for some problems. And yet, crafty thieves can sometimes get their information directly from you. Ways you may unwittingly give them access include:

- Throwing away account statements and receipts with your full account number listed. Also, tossing pre-approved credit card offers that come in the mail (which have your name and address all over them). Identity thieves know that "dumpster diving" can yield a bounty of personal information. So shred or tear up these items before you trash them.
- Giving them your credit or debit card numbers in a practice known as "skimming." Thieves may swipe your card for an actual purchase through their own data storage device, or attach the device to an ATM machine where you swipe your card. This is harder to protect against, but your best bet is to avoid letting your card out of your sight during a transaction.
- Giving out your information over the telephone. Known as "pretexting," thieves call to tell you there's a "problem" with one of your financial accounts. Then they ask for your account number or other personal information to "verify" your identity. Any legitimate company that you have an account with may call to discuss your account and need to verify your identity, but will do so in ways other than asking for your personal information (e.g., your mother's maiden name). Still, protect yourself by asking for a number at which to call the person back, then calling the company's customer service number to find out if there really is a problem with your account.

When it comes to the Internet, people tend to worry about the security of making online purchases. But the bigger danger is, again, unintentionally giving criminals your personal information. Some popular schemes include:

Phishing can appear in the form of an E-mail or pop-up message. It looks like it's from a credit union, bank, credit card company, or online store, indicating that there's some type of "problem" with your account. This time, the E-mail or pop-up message prompts you to click on a link to "update" or "verify" your information. **Don't do it.** Legitimate companies never ask for this information via E-mail or pop-up message. If you're concerned that a company is actually trying to contact you, call it directly instead, using a phone number listed on your monthly statement or the company's Web site. You can also forward phishing E-mails to **spam@uce.gov** and to the organization impersonated.

Free software or ***freeware*** can also be a scam to get your personal information. While any type of free software can pose a problem, file-sharing software is particularly problematic. Yes, it can give you access to a wealth of goodies such as music and games, but sometimes it comes loaded with a bad bonus—a criminal's free rein of your computer. If you don't check the software's sharing permissions (usually found under the "Properties," "Preferences," "Options," or "Settings" menus), you may unknowingly provide access to your entire hard drive—including tax returns, E-mail messages, medical records, photos, or other personal documents. Not all free software is bad, but you do have to be careful. If you decide to download it, set it up carefully and take the time to read the end-user licensing agreement to be sure you understand what you're saying yes to by using the software.

Spyware is a bad side effect of free downloads—even those forwarded by friends or sent by businesses you know. Some downloads install spyware onto your hard drive without your consent, which monitors or controls your computer use. Spyware may be used to send you pop-up ads, redirect your computer to unwanted Web sites, monitor your Internet surfing, or record your keystrokes, which can lead to identity theft. The best way to avoid spyware is to resist the urge to install any software unless you know exactly what it is and the reputation of the company offering it. And if your anti-virus software doesn't include a spyware blocker, install separate anti-spyware software, use it, and learn how to update it regularly.

Exercise 5H:
Luring You In

Read the messages below. You might view these or similar messages when you surf the Net or read E-mail. How do you think each message might be used in a deceptive way?

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"The bank's technical department is performing a scheduled software upgrade to improve the quality of its services. By clicking on the link below, you will begin the procedure of the user details confirmation."

"You've won a free copy of xxxx software! Click here to begin your free download."

Exercise 5I:

Deal With Deception

What would you do if you suspected that someone might be trying to deceive you? Respond to scenarios that involve suspicious behavior. In each situation, describe what you should do to avoid or deal with the suspicious activity.

1. **You walk up to an ATM and a guy walks up behind you who appears to be waiting his turn. But he's uncomfortably close—right over your shoulder—as you get ready to enter your PIN.**

2. **You're at a cash register in a store and have given the clerk your credit card. She holds on to it, probably to verify your signature. But then she says she needs to grab something from the back and starts to walk away with your card in hand.**

3. **A caller says she's from your credit card company and wants to offer you a higher credit limit for being such a good customer. You reply, "Great, what do I have to do?" And she tells you to give her your Social Security number for verification.**

4. **You've found a pair of shoes at a great price on a Web site you just found. You start the check-out process and notice that the padlock at the bottom of your computer screen is open and that the Web page address starts with "http" instead of "https."**

5. **You get an E-mail from an online bookstore you frequently buy from. It says that the credit card on your account has expired and gives you a link to update your information.**

6. **Your friend sends you an E-mail about cool new software that lets you share music with others for free. He sends you the link to download the software, which is from a site you've never heard of.**

7. **You're bummed out about losing in an online auction. But then you get an E-mail stating the winner backed out and that you can have the item if you still want it, and to just send your credit card information via E-mail.**

So how do you keep your personal information secure in the midst of all these threats?

Ten smart steps to take are:

1. Don't leave your wallet or credit card statements lying around—even at home. The Federal Trade Commission (FTC) estimates that one in four victims knows the identity thief.

2. Sign new credit cards as soon as you receive them, cut up and discard expired cards, and shred or tear up unwanted "pre-approved" credit card applications.

3. When you sign receipts, draw a line through any blank spaces above the total. Save your receipts until you reconcile them with your statement, then either rip them up or keep them and any carbon copies in a safe place.

4. Never give your credit card number or Social Security number to anyone over the phone unless you initiate a call to a business to discuss your account. And never send these numbers by E-mail—it is rarely secure.

5. Always keep PINs for your credit and debit cards completely confidential. Don't write PINs on your cards or carry them with you.

6. Review all of your monthly statements carefully, and report unauthorized charges and other activity immediately.

7. When it's time to clean out your financial files, shred anything that has your Social Security number or credit card numbers on it.

8. On your computer, install and use firewall, anti-virus, and anti-spyware software, and learn how to keep them all up to date.

9. Don't fall for phishing or pretexting scams. Legitimate businesses that contact you should not have to ask for your account number or Social Security number. If you think there really might be an issue with an account, get a customer service number from your statement, and call the business back.

10. When you buy something on the Internet, check that the page is secure before entering your credit card number. You should either see an icon of a closed padlock  or unbroken key  in the bottom browser bar or that the site's address begins with "https" (notice the "s") to show it's secure.

Despite all your best efforts, the worst may still happen. Maybe your wallet gets stolen with your Social Security card inside it. Or you get a letter from a company stating that your information may have been accessed by a hacker. Placing an initial fraud alert on your credit report can help prevent an identity thief from opening any more accounts in your name.

To place the alert, call the toll-free fraud number of any one of the three nationwide credit reporting bureaus—Equifax, Experian, and TransUnion—and tell the bureau you suspect you have been, or are about to become, the victim of identity theft. You'll have to provide appropriate proof of your identity, which may include your Social Security number, name, address, and other personal information requested by the credit reporting agency.

Luckily, one call does it all—the credit reporting agency you contact must contact the other two. Then each agency must place an alert on its version of your report. For the next 90 days, businesses will see the alert on your credit report and must verify your identity before issuing credit in your name—which usually means contacting you directly.

Once you place the alert, you'll get information about ordering a free credit report from each of the credit agencies. Your best bet, though, is to wait about a month from the time your information was stolen before you order the reports because suspicious activity may not show up right away. Once you get the reports, look for questionable activity such as inquiries from companies you didn't contact, accounts you didn't open, and debits on your accounts that you can't explain. Also check that information like your Social Security number, address(es), your name, and your employer's name is correct. Continue to check your credit reports periodically over the next year to make sure no new fraudulent activity has occurred.

If you do find that your information has been misused, immediately close any compromised accounts and file a police report. This report is proof of the crime and may be important to have later—the credit reporting agencies usually require it when you place an extended fraud alert on your credit reports. You should also file a complaint with the FTC at **www.ftc.gov/idtheft.** This can help law enforcement officials across the country in their identity theft investigations.

Assignment 5-5:

Online Warnings

Create an alert notice that can be posted near your computer at home or near the computer stations at the local library. This notice should give Internet users tips on how to avoid or deal with suspicious online messages.

Assessment 5-1: Using Financial Services

Use what you learned in Unit 5 to practice selecting and dealing with various financial services. Show what you have learned by reflecting on how financial services fit into your financial plan.

Adding It Up

We've covered a lot of topics in this unit, all related to the theme of financial services. You've learned about various types of financial services providers you may need. You should know the ins-and-outs of using basic services—from savings and checking accounts to debit and credit cards—to manage your money more efficiently. And you now understand how automated services can make life much easier.

Of course, we also visited the dark side of financial services—identity theft. Although not a fun topic, it's an important one. And now you should have a better idea of how to prevent it and how to respond if it does happen to you.

Next, we'll talk about another way to protect your wallet. This time, though, it's protecting yourself from big losses with insurance.

For more tips, tools, and articles about financial institutions, visit hsfpp.nefe.org.

Unit Assessment 5-1: Using Financial Services

Use what you learned in Unit 5 to practice selecting and dealing with various financial services. Show what you have learned by reflecting on how financial services fit into your financial plan.

Competency:
Demonstrate how to use various financial services.

Directions:

- ☐ Preview the Required Criteria to plan your activities for this assessment.
- ☐ Complete the unit assignments as assigned by your instructor.
- ☐ Write two to three paragraphs to reflect on how financial services fit into your financial plan so you meet your financial goals. For example, consider how and which services can help you stick with your budget or be used for saving or investing goals.

Required Criteria	Status
1. You use the decision-making process to compare providers of financial services [Assignment 5-1]	complete not complete
2. You use and reconcile a checking account over a two-month cycle [Assignment 5-2]	complete not complete
3. You use the decision-making process to compare credit card plans [Assignment 5-3]	complete not complete
4. You share what you learned about a trend in online financial services [Assignment 5-4]	complete not complete
5. You create a notice to alert others about how to deal with deceptive online practices [Assignment 5-5]	complete not complete
6. You write two to three paragraphs reflecting on how financial services fit into your financial plan	complete not complete
7. You specify at least three criteria related to financial services that you need and/or want now and in the near future	complete not complete
8. Your reflection paragraphs include a list of financial services that apply to your current and near-future situation	complete not complete
9. You summarize strategies you will implement to be a wise user of financial services	complete not complete

Feedback:

Score _____/20 **Name** _____ **Date** _____