39th Annual Community Bank Week
2017 Theme:

Here you will find:

- Celebration Ideas from other Community Banks
- Governor's Proclamation
- Letter to the Editor
- Press Release (coming soon)
- Statement Stuffers
- Coloring Pages
- Financial Literacy Information

How to Use Your Kit for Community Bank Week: 6 Easy Ways!

Governor's Proclamation
Post the Proclamation in your bank lobby (perhaps place it in an inexpensive 8 1/2 x 11 photo frame). The proclamation explains the importance of community banks to the Kansas economy and announces the official 2017 statewide celebration.

Coloring Contest
Children's activities always create attention - so here's how to get the kids involved in Community Bank Week. First you need to fill in the blanks on the rules page. Once that is done, make copies of the coloring page and copy the contest rules on the back of the page. Have them color it, fill out the information on the rules sheet, and return to the bank by a certain date. Display them in the lobby, have judges pick out the best one from each age group, and have prizes of savings bonds etc., and/or give a prize to all that enter the contest.

Sample Letters to the Editor
A free, inexpensive and effective way to explain your bank's importance to the community economy. We've made it easy too! Simply retype one or both of the letters on your bank's letterhead, filling in your bank and community information in the proper spaces. Then deliver to your local newspaper to be printed. Research has shown letters to editors are well read and effective. We also recommend that you type the letter and email it directly to your local editor, as this makes it easy for them to print it!

***Note**: If there are several CBA members in your county, (consult your membership directory) you may want to jointly sign the letter.*

News Release on Kansas Community Bank Week
Not much work here - just type the press release on your bank's stationery, take it to the newspaper personally, and ask the editor to run it the week of April 24th – 29th, 2017. You can also add a tag line at the end of the article. It could say something like - "[insert your bank name] is a member of the Community Bankers Association of Kansas."

***Note:** Emailing the press release to your local news outlets is also a great idea. Try radio in addition to print.*

Like to talk about community banking? So do we. Contact your local talk radio station to ask if you can participate in a morning talk show or other opportunity. Many times, radio stations welcome the opportunity to fill a space with a great discussion - and make sure to send them the press release when you call to set up the interview. This is also an exciting way to offer community members a chance to call the station with their questions during the interview.

Host a media reception at your bank during Community Bank Week. Ask your local media to come via a printed or emailed invitation. Let them know you're sharing information about the importance and impact of community banking, and that you're

inviting media for a “behind the scenes” tour. Prepare a fact sheet in advance of how community banking impacts so many areas of the local community. Assign someone in your bank to lead the tour, and have them read the official Proclamation as a highlight of the event. You can combine this with your customer celebration for added impact.

STATE OF KANSAS

PROCLAMATION BY THE GOVERNOR

TO THE PEOPLE OF KANSAS, GREETINGS:

WHEREAS, the tradition of locally owned and operated banks in this state helped generate a state with diverse business and industry to the betterment of its citizens; and

WHEREAS, the primary focus of Kansas community banks continues to be the prosperity of individuals and small businesses in their hometowns. Community banks within their own communities, providing residential mortgages, small business loans, agricultural loans, and many types of consumer loans for families and individuals; and

WHEREAS, community banks play a significant role in local economic development efforts of Kansas communities stimulating the economy to produce jobs and new opportunities; and, as a group, continue to contribute an important and vital link in the state's economy; and

WHEREAS, the directors, officers and employees of Kansas community banks are champions of their local communities. Their high involvement in their local communities, typifies the dedication and community citizenship that is part of the tradition of community banking:

NOW, THEREFORE, I, Sam Brownback, GOVERNOR OF THE STATE OF KANSAS, do hereby recognize April 24-29, 2017, as

Kansas Community Bank Week

in Kansas.

DONE: At the Capitol in Topeka
under the Great Seal of the
State this 17th day of
February, A.D. 2017

BY THE GOVERNOR: Sam Brownback

Secretary of State

Assistant Secretary of State

CBW Celebration Ideas:
Community Bank Week is April 24-29, 2017

CBA has been asked how other Kansas banks celebrate Community Bank Week (CBW). Below is a compiled list of ideas from banks that have participated in CBW in past years and have shared their successful suggestions.

Local Media Opportunities:

Advertise - Place ads about your CBW celebration in the local newspaper and on radio stations. You can also use other advertising opportunities, such as community bulletin boards, schools, flyers and other grassroots connections. These are great ways to advertise for free. When holding your special event, don't forget to invite your local newspaper and radio station!

In Your Bank and For Your Customers:

Create a Pin Wall - Place a large map of your area (or the state of Kansas) in your lobby. Have pins and post-it notes available nearby. Ask customers to answer questions, like "How long has your family lived here?" or "Where is your favorite place to eat?" and have them mark that area with a post-it note answer and a pin. Post a sign above the map that says "Find out how our region is part of a 'roadmap to success' for area customers."

Theme Week - Attract attention to your bank by featuring a theme for each day of the week: this year's CBW theme is "Your Roadmap to Success!" HINT: Use Kansas maps, map-themed activities, scavenger hunts, highlight your area's town stories and legends, (such as things that make your "road" unique), or host a "road trip" themed day.

Drawings - Each day, give away something to your customers: tickets to the local basketball game, free family photo package at your local photographer, a family pass to the local pool and other items that encourage community spending. This is also a great way to highlight area organizations that conduct their banking business with you. You may want to consider giving items that make a "great day out" in your region to fit the roadmap theme – such as local museum or restaurant passes.

Host a "Tailgate" - Decorate the bank lobby with local high school or college team colors, have hamburgers and hot dogs and a prize table for the visitors to select novelty prizes: foam fingers, footballs, baseballs, tennis balls, soccer balls, etc…

Health Day - Offer mini physicals; blood pressure, cholesterol, hearing and vision checks.

Protect Your Identity - Have a shredder on hand for customers to shred personal items. Hold a drawing during the day for the winner to take home a personal shedder. Hand out Identity Theft information to everyone who comes in.

Raffle - Have three or four big items to raffle: iPad, TV, Royals Tickets, KSU or KU Game Tickets. Use the proceeds to donate to your local 4-H Club, Boy or Girl Scout

Troop or your local sports team. Idea: Use items from local businesses that have loans or accounts with your bank as the featured giveaway items!

Coloring Contest - For younger children (preschool through third grade) have a coloring contest, for different age groups. Give each child a small gift to take home with them. At the end of the week give your winners $50 towards their very own savings account. Be sure to show off all of your entries!

Pennies in a Jar - For kids a bit older: have different age groups guess how many pennies are in the jar. At the end of the week give your winners pool passes or movie tickets.

Display – Showcase arts and crafts or town memorabilia in your lobby, from local artists and high-school students. It's a great way to involve your entire community.

Scavenger Hunt - Each day post clues in your bank and on your phone message. The one who finds the prize wins: a gift certificate, cash or tickets to a College Baseball Game. Because the theme is "roadmap," you can include clues for scavenger hunt stops nearby your bank!

Spirit Day - Decorate your bank with school's colors and mascot: give each person that comes in kool-aid, popcorn and/or cookies.

First Deposit Program: Encourage families to come and open accounts with their child. Announce that during CBW, if you open an account with $25, you'll add $10 to it.

Get Your Local Community Involved:

Host an Essay Contest – Have students in grade school through high school write an essay about what "community" means to them … or why community banks and community businesses are a "roadmap to success." Share the top essays at a school and parent reception. Give away a $100 savings bond for the top essay, and invite all participants to come and read their essays during the reception. (Parents and grandparents enjoy this!)

Bake Sale – Set up a bake sale to benefit your local schools. Sell themed goodies: school colored cupcakes, bags of popcorn, Kansas-shaped suckers or cookies, etc…

Sports Themed Costume Contest – Host a costume party and have your customers dress up in their favorite team gear: jersey's, face paint, cheerleader gear, pom-poms, etc… Have a judge and a grand prize winner!

Contributions - Host a community fundraiser, and encourage your community to donate food, clothing, coats and toys to those less fortunate. Give each participant a small gift.

Limo Ride - Get teenagers involved! With prom right around the corner, what better than a contest that gives the winner a limo ride to and from the prom?

Tour Time! - Invite all of the second, third, or fourth graders from your local elementary school in for a bank tour. Let them visit each area or department of the bank. You could have them step inside the vault, let them view old and new currency and talk about the banking process. Give each child a small souvenir.

Patriotic Day - Start by having local elementary children write letters or make cards for soldiers overseas. Be sure to display all letters/cards throughout the week. Designate a day in the bank to invite people in the community to the bank for apple, cherry and blueberry pie with red or blue punch. Be sure to wear your red, white and blue that day!

Safety Day - Ask your local sheriff's office to come in to perform car seat checks and to do child I.D. and finger printing. Hand out safe driving tips to teenagers. Invite fire trucks and police cars to come to the parking lot for visits with children.

Beautification Day - Hand out flower seeds while your employees donate their time to clean up your community. Pick up litter, paint park benches, plant trees or adopt a house in your neighborhood that needs a little TLC. You can put a computer-printed label on each seed packet with your bank name and logo and the theme for Community Bank Week, "Your Roadmap to Success."

Senior Citizens - Host a lunch for local seniors; have bingo, card games and other fun things. Host a 'senior' prom: have dinner and dancing. Don't forget to take pictures!

Host a video contest. Ask local students to prepare a YouTube video highlighting how community banks help their town remain successful. Offer a prize to the school with the best video, and show all the videos at an in-bank reception. Share these videos on social media if you have active accounts for your bank. CBA will share top videos on our website also! Idea: You can have fun with this by having parents ask kids in the video how much things cost, how much it costs to live, etc.

Host an art gallery in your bank. Ask local students to prepare specific artwork to display that shows what's unique or special about your community. Invite the parents and the public to an Art Gallery Exhibit evening. Allow members of the community to form a volunteer "jury" and give a ribbon to the best entries. Give the exhibit a theme, such as "the view from our roadmap to success."

CBW 2017 – Bank Press Release
Attention Member Banks:
Please edit this copy to suit your banking situation….

1. **RE-TYPE** this draft on your bank's stationery, **INCLUDE** bank name and appropriate bank officer's name where indicated along with your edits. Add or **REMOVE** text as you feel appropriate.

2. **DELIVER** to your local newspaper office(s) before the week of Kansas Community Bank Week, April 24th – 29th. Remember to check your newspaper's deadline. A good goal is to deliver the piece one full week in advance (on or by April 17th).

3. **IF YOU SHARE** the same local newspaper with other CBA Members in the area, please consider adjusting it to include all area CBA member banks so as to avoid duplication.

For more information contact:
(**Bank Contact**)
(**Bank Name**)
(**Phone Number**)
For Release Between April 14th - April 21st, 2017

CBA and [COMMUNITY BANK NAME HERE] Recognize Community Bank Week April 24th- 29th, 2017

Week Set Aside to Celebrate the Unique Impact of Community Banks on Local Businesses, Families and Communities

CITY, STATE (April XX, 2017) — Community banks are part of the essential fabric of the rural or urban areas they call home. Inside these doors, critical decisions are made daily to ensure the success of local businesses, families, schools and communities. Across the state of Kansas, April 24th – 29th, 2017, is set aside to celebrate and recognize Community Bank Week. Members of the Community Bankers Association of Kansas (CBA) including **[BANK NAME, CITY, STATE]** are hosting several activities to honor the vital role that community banks serve in their cities and towns.

"Community banks exist to come alongside local businesses and families to see their goals and dreams become reality," said Blake Heid, CBA Chairman and President/CEO, First Option Bank, Paola, KS. "Across Kansas, nearly 300 community banks open their doors daily with a shared goal of seeing their local rural and urban areas succeed. The driving force of their daily decisions are always community bank customers, and CBA Community Bank Week gives community banks a chance to say 'thank you' in creative ways."

Hundreds of community banks across Kansas recognize CBA Community Bank Week in

unique ways, including in-bank customer events, media events and partnerships with local organizations or schools. Past CBA Community Bank Week activities have included partnerships with local charities or activities to promote economic development initiatives. Many community banks traditionally mark the week by highlighting their community service or financial education programs. **[ADD A SENTENCE OR TWO ABOUT WHAT YOUR BANK IS DOING].**

"CBA Community Bank Week is special because it offers us the chance at **[BANK NAME]** to celebrate our community and our customers," **[BANK OFFICIAL, TITLE, BANK NAME]** said. "Customers of community banks know they'll receive top-notch expertise on critical issues, but they also know that we'll know them by name. We genuinely care about what matters to them. Here in **[TOWN NAME]** we are committed to taking the steps each day to maintain our community's economic success."

About CBA

Community Bankers Association of Kansas serves independently owned and operated banks of all sizes and charter types throughout the state of Kansas offering political representation, educational training and networking opportunities. Their purpose is to promote the economic strength in Kansas community banks. For more information, visit www.cbak.com.

# # #

CBW 2017 – Bank Press Release
Attention Member Banks: Please edit this copy to suit your banking situation….

1. **RE-TYPE** this draft on your bank's stationery, **INCLUDE** bank name and appropriate bank officer's name where indicated along with your edits. Add or **REMOVE** text as you feel appropriate.

2. **DELIVER** to your local newspaper office(s) before the week of Kansas Community Bank Week, April 24th – 29th. Remember to check your newspaper's deadline. A good goal is to deliver the piece one full week in advance (on or by April 17th).

3. **IF YOU SHARE** the same local newspaper with other CBA Members in the area, please consider adjusting it to include all area CBA member banks so as to avoid duplication.

For more information contact:
(**Bank Contact**)
(**Bank Name**)
(**Phone Number**)
For Release Between April 14th - April 21st, 2017

CBA and [COMMUNITY BANK NAME HERE]:
Community Banks Central to Rural Economy; Multi-Million Dollar Impact Recognized During Community Bank Week

CITY, STATE (April XX, 2017) - Across the state of Kansas, more than 300 community banks serve local customers, businesses and families each year – resulting in a multi-million dollar impact on the rural economy. During the week of April 24th – April 29th, 2017, Community Bankers Association of Kansas (CBA) and **[BANK NAME, CITY, STATE]** recognize CBA Community Bank Week and honor this impact with several activities at the local bank level.

"Community banks work alongside businesses, families and agricultural producers in hundreds of Kansas communities – both rural and urban – by meeting their financing and planning needs," says Blake Heid, CBA Chairman and President/CEO, First Option Bank, Paola, KS. "During Community Bank Week, we celebrate and honor that critical mission and how it sustains the future of Kansas towns themselves."

Community banks contribute to rural economies in a numerous ways, including helping establish opportunities for local jobs, maintaining the local tax base and facilitating development of the infrastructure and public services necessary to keep rural communities strong. Across the commercial banking sector, community banks remain the

largest provider of agricultural credit. They often serve as a key partner for new and expanded business opportunities, which in turn fuels community schools and growth.

"Community banks like **[BANK NAME]** access key resources like government loan programs for housing or small business and farm loans to help individuals, families and businesses achieve the credit needed to move forward," **[BANK OFFICIAL, TITLE, BANK NAME]** said. "Ultimately we are driven by the individual goals and needs of our customers. This is a unique feature of community banks, and we're proud to offer high-impact tools for our customers' continued success – but in a very personal, meaningful way. Community Bank Week honors that commitment."

Each year, community banks across Kansas recognize CBA Community Bank Week in a variety of ways. Celebrations include special events with local charities, community-based in-bank events and promoting economic development initiatives. Many banks offer programs to boost financial literacy in partnership with civic entities. Learn more about activities planned by **[BANK NAME]** today by calling **[BANK NUMBER].**

About CBA
Community Bankers Association of Kansas serves independently owned and operated banks of all sizes and charter types throughout the state of Kansas offering political representation, educational training and networking opportunities. Their purpose is to promote the economic strength in Kansas community banks. For more information, visit www.cbak.com.

##

CBW 2017 – Letter to the Editor
Attention Member Banks: Please edit this copy to suit your banking situation….

1. **RE-TYPE** this draft on your bank's stationery, **INCLUDE** bank name and appropriate bank officer's name where indicated along with your edits. Add or **REMOVE** text as you feel appropriate.

2. **DELIVER** to your local newspaper office(s) on or before the week of Kansas Community Bank Week, April 24th – April 29th, 2017. Remember to check your newspaper's deadline.

3. If you are **JOINTLY WORKING** with other CBA Members in the area (if you all share the same local newspaper), consider adjusting it to be signed by each of the bank's CEO. This letter is designed and **PERMITTED FOR USE ONLY** by CBA Members.

Dear Editor:
In April, we ask readers to consider the activity happening inside the 300 community banks across the state of Kansas. This truly supports and fuels our economy, but it happens on a very personal level that is hard to find today. Community bankers throughout the nation will celebrate April as Community Bank Month. In Kansas, Governor Sam Brownback has proclaimed April 24th – 29th as Kansas Community Bank Week.

(*Name of Bank*) will join other members of the Community Bankers Association of Kansas (CBA) to increase awareness of the crucial role community banks play in the nation's economy and the local economy. This includes special events and activities to demonstrate to our customers our commitment to meeting their needs in a unique and personal way.

Events this year center around the theme "Your roadmap to success." We believe this theme represents all the ways local banks guide customers toward their dreams and goals and help communities themselves remain connected and strong. Not only do community banks fuel the financing and loan services that move businesses and families forward, we know our customers' names. We know their goals. We know how they make a difference in our own towns.

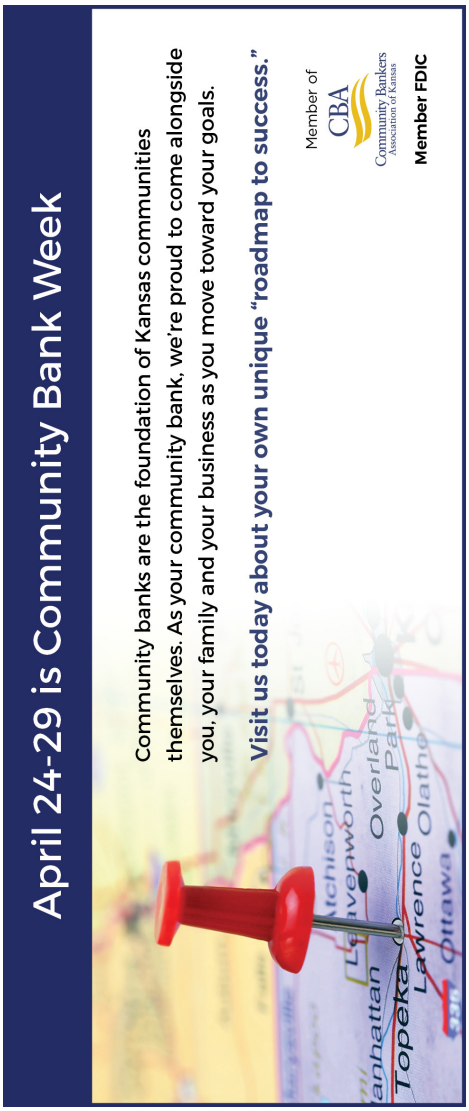
In fact, (*Name of Bank*) has been owned and operated locally since (*year of bank charter*). Rather than shifting our funds away from local economies as the "big banks" do, (*name of bank*) channels most of our resources toward loans within our neighborhood where our depositors live and work. These local deposits impact the economy by developing small businesses, purchasing and repairing homes and financing college educations. They also help create jobs and promote education – critical elements of a strong local future.

(*name of bank*) officers and employees represent the nature of a true community bank. We live in the same neighborhoods as our customers, shop in the same stores, attend the same churches and the same schools. This means our work toward local reinvestment remains our primary focus for bank decisions and policies. We wouldn't have it any other way. We take pride in really knowing our customers and coming alongside them in their continued success, every step of the journey.

As we celebrate Kansas Community Bank Week, April 24th -29th, we invite all your readers - our friends and neighbors - to stop by our bank(*s*) and let us thank them in person for their partnership and trust in (*bank name*) to serve this community.

Yours truly,
(Please have officer sign letter prior to delivery to your newspaper.)
Your Bank Officer's Name
Title
Bank Name and Address

How to use your statement stuffers:



The originals are enclosed in this packet.

You can place them in your customers' bank statements and/or hand them out at the teller window. These statement stuffers are a great and inexpensive way to advertise the importance of your bank to the community. All you have to do is place your bank logo, stamp, etc. in the blank space in the middle of each stuffer, cut, and then hand out.

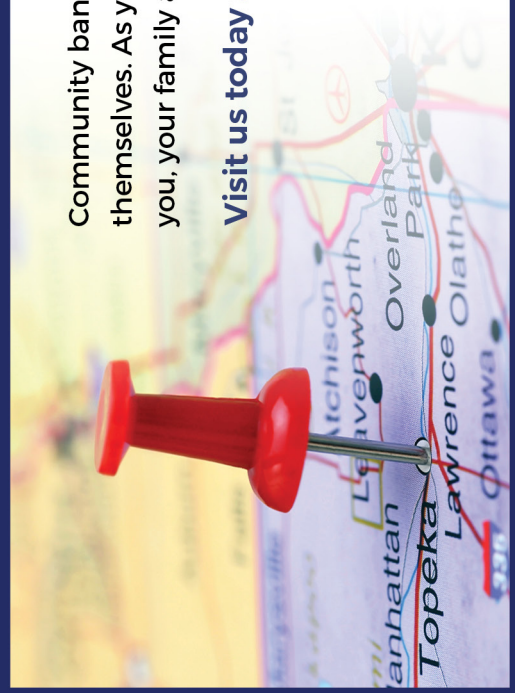
April 24-29 is Community Bank Week

Community banks are the foundation of Kansas communities themselves. As your community bank, we're proud to come alongside you, your family and your business as you move toward your goals.

Visit us today about your own unique "roadmap to success."

Member of CBA Community Bankers Association of Kansas

Member FDIC



Community Bank Week
April 24-29, 2017

A **true** Kansas Community Bank is based on a strong commitment to people. As your needs and dreams change for your family and your business, we're with you every step of the way. We would like to show you our appreciation.

Please stop by the bank
April 24th – 29th
during Community Bank Week.

Member FDIC

Member of Community Bankers Association of Kansas
Representing Community Banks

APRIL 24-29 IS COMMUNITY BANK WEEK

As your community bank, we are celebrating the success of our community. Stop by and help us celebrate – and don't forget to check out all our other services too! Find out how we can be part of your unique "roadmap to success."

Member of CBA Community Bankers Association of Kansas

Member FDIC

Coloring Contest Rules

1. Only children between the ages of _____ and _____ may participate.
2. Children of this bank's employees are NOT eligible for the contest.
3. All entries are due by 5 p.m. on _____.
4. The judge's decisions are final.
5. The following prizes will be given (savings bonds, ad specialty items, etc.)
   -
   -
   -
   -

IMPORTANT INFORMATION

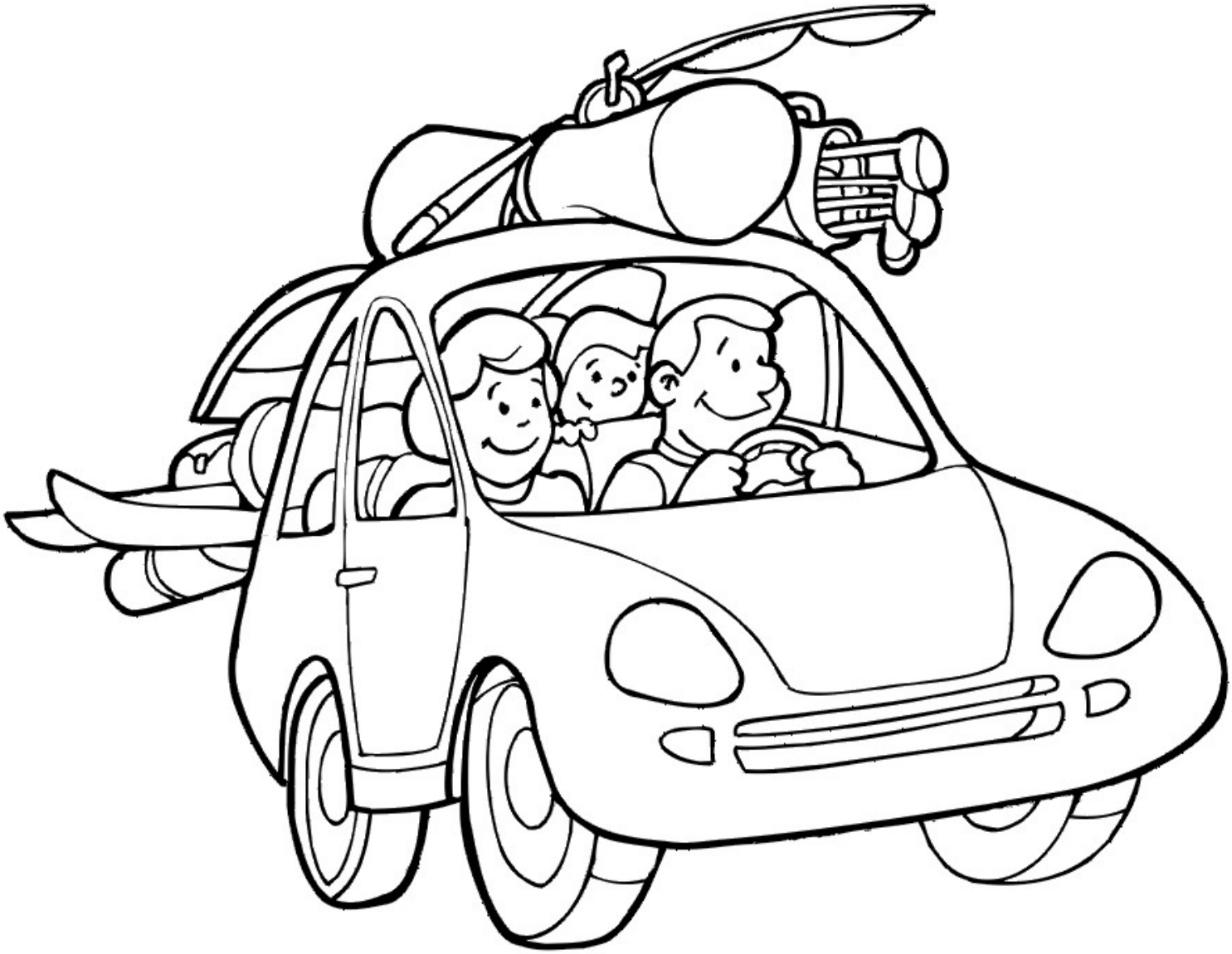
Entrant's Name_____ Age_____

Address:_____ Phone_____

Parent's or Guardian's Signature_____

Community Banking: Your Roadmap to Success

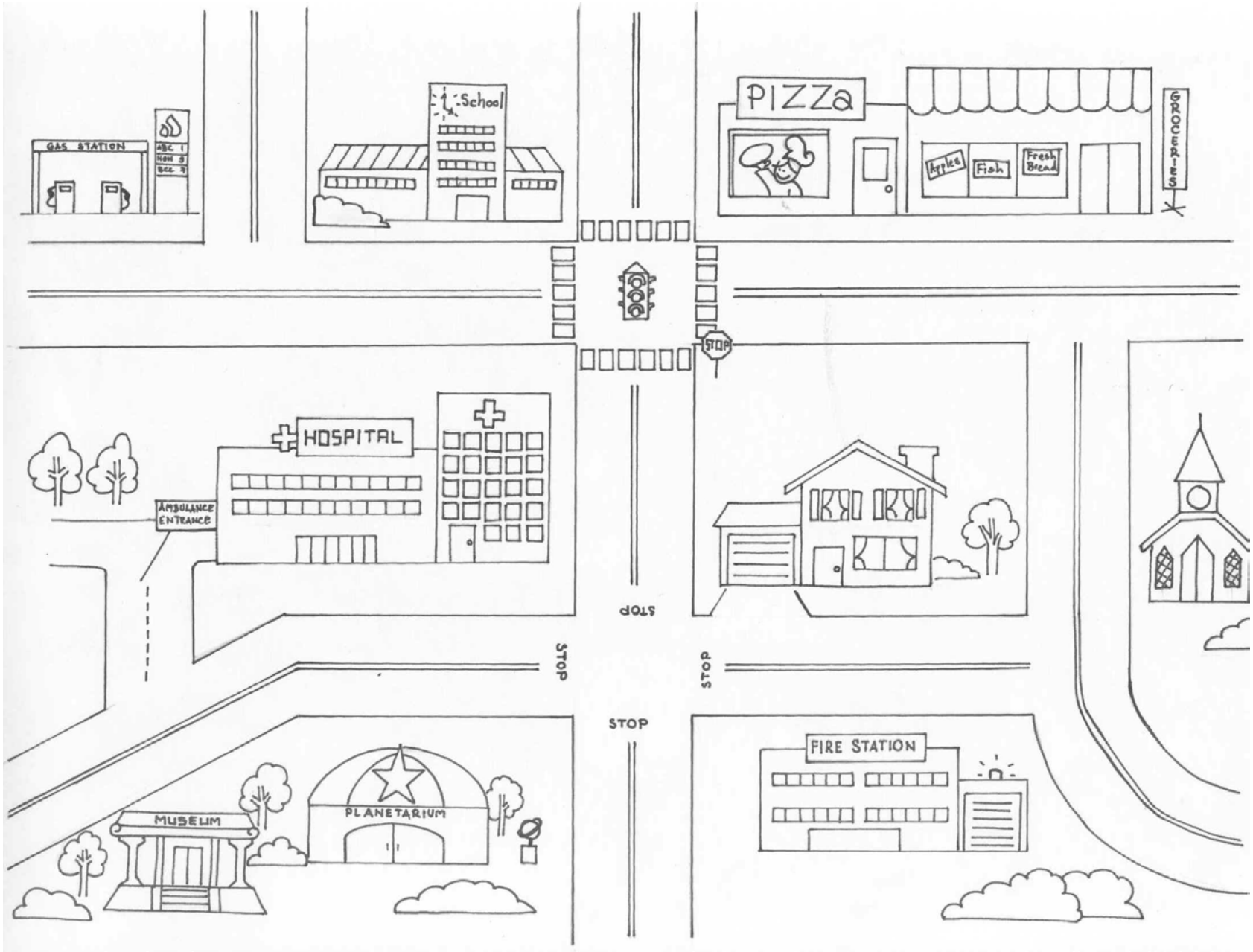
Kansas Community Bank Week April 24th – 29th



COLORED BY: _____ AGE: _____

Community Banking: Your Roadmap to Success

Kansas Community Bank Week April 24th – 29th



COLORED BY: _____ AGE: _____

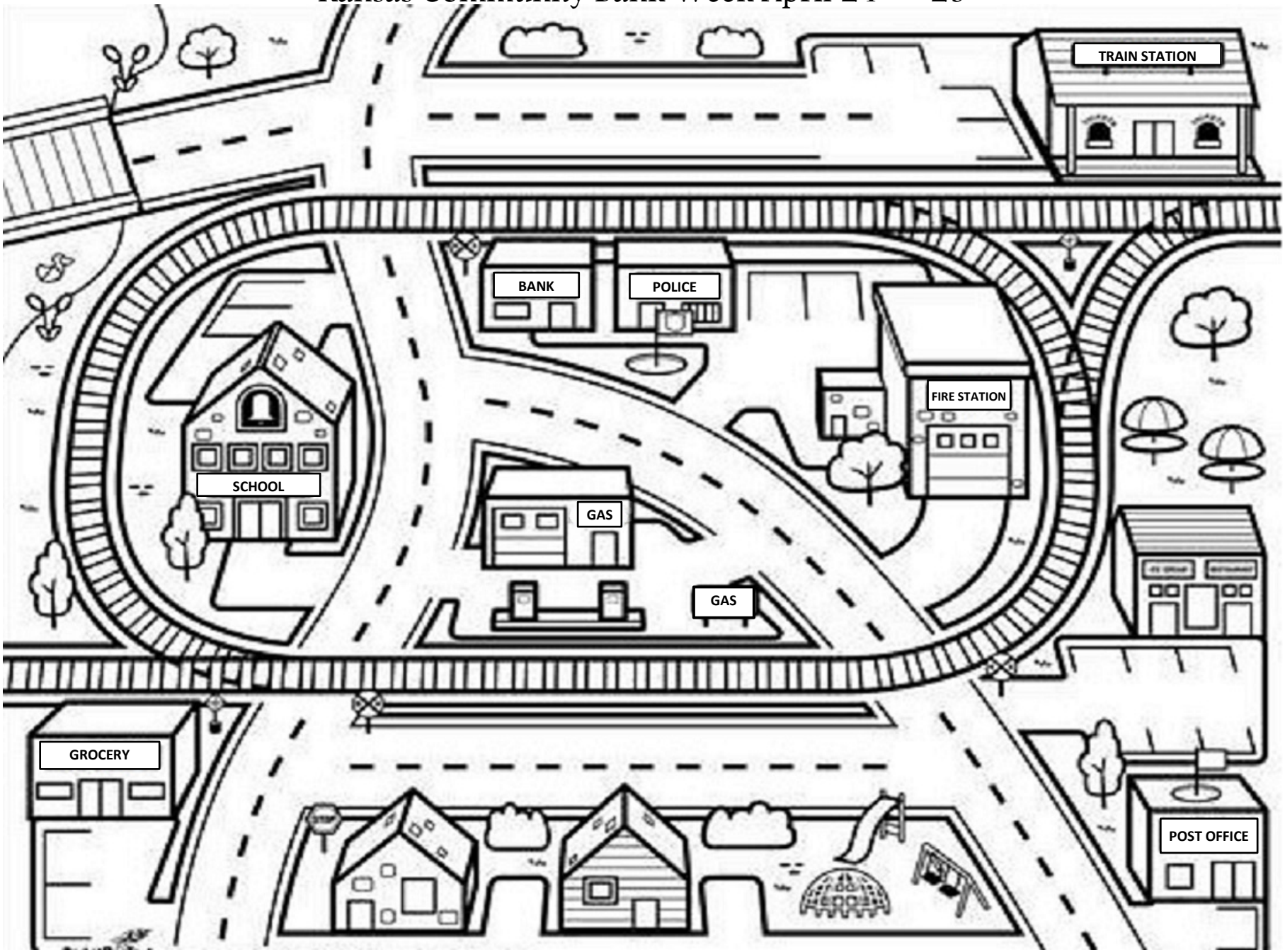
Community Banking: Your Roadmap to Success

Kansas Community Bank Week April 24th – 29th

COLORED BY: _____ AGE: _____

Community Banking: Your Roadmap to Success

Kansas Community Bank Week April 24th – 29th



COLORED BY: _____ AGE: _____

Community Banking: Your Roadmap to Success

Kansas Community Bank Week April 24th – 29th

COLORED BY: _____ AGE: _____

IN TIMES LIKE THESE WE REALLY NEED HEROES

Meet **THE CENTSABLES**, a multi-media program that's helping kids everywhere acquire real-life money management skills. Their mission: to establish you as a leader in supporting financial literacy.

A TURNKEY OPPORTUNITY OF HEROIC PROPORTIONS

The program helps you build positive PR and deliver value-added service, faster than a speeding bullet! The Centsables reach - and teach - kids in the ways they like most:

- interactive website
- mobile financial fitness tour
- ground breaking animated TV series
- animated PSAs
- classroom module
- proprietary banking for kids program
- financial literacy board game
- comic book series
- Factivity workbooks
- action figures

TAKE 5 MINUTES TODAY. IMPROVE TOMORROW FOR KIDS

Please visit www.centsables.com, to explore our public service version of the website, currently being offered as a resource for parents. Then contact us, to discuss sponsorship opportunities, and the ways The Centsables program can be customized to your goals.

EMAIL US TODAY AT INFO@CENTSABLES.COM
AND BECOME A HERO IN THE COMMUNITY YOU SERVE!

ADDITIONAL RESOURCES

For more information on creating and maintaining a budget, visit
www.practicalmoneyskills.com/budgeting

For an online Budget Worksheet that calculates the figures for you, visit
www.practicalmoneyskills.com/budgetplanner

For additional online calculators, visit
www.practicalmoneyskills.com/calculators

Practical Money Skills for Life™

For more information, visit
www.practicalmoneyskills.com

VISA

Practical Money Skills for Life™

PRACTICAL MONEY GUIDES

BUDGET BASICS

Learn to create and stick to a budget

VISA

IT'S EASY TO CREATE A BUDGET THAT WORKS FOR YOU

A budget can help you pay your bills on time, cover unexpected emergencies, and reach your financial goals—now and in the future. Most of the information you need for your budget is already at your fingertips. This guide explains how to create a budget and stick to it.

PRACTICAL MONEY GUIDES

BUDGET BASICS
CREDIT HISTORY
CREDIT CARD BASICS
DEBIT CARD BASICS
PREPAID CARD BASICS
IDENTITY THEFT

When you understand how to manage your finances, you've got an invaluable tool in taking control of your life. Wise use of these skills can provide peace of mind, financial freedom, increased buying power and a secure future. This guide is one of a series on **PRACTICAL MONEY SKILLS FOR LIFE.**

CREATE YOUR BUDGET

This worksheet will help you get a clear picture of your monthly finances. It will also act as a starting point for your budget. To complete it, follow the simple steps outlined below.

1. QUESTION YOUR NEEDS AND WANTS What do you want? What do you really need? Evaluate your current financial situation. Take a look at the big picture. Make two lists – one for needs and one for wants. As you make the list, ask yourself:

- Why do I want it?
- How would things be different if I had it?
- What other things would change if I had it? (for better or worse)
- Which things are truly important to me?
- Does this match my values?

2. SET GUIDELINES We all have different budgets based on our needs and wants. But the Building a Budget chart on the next page shows some guidelines on how much should go toward different expenses. You may need to make adjustments for a daily latte fix or visits to family, but remember to subtract amounts from other areas if you do.

3. ADD UP YOUR INCOME To set a monthly budget, you need to know what's coming in. Make sure you include all sources of income such as salaries, interest, pension, and any other income sources.

4. ESTIMATE EXPENSES The best way to do this is to keep track of how much you spend each month. Categorize spending depending on your needs and wants. Use the Budget Worksheet in this guide as a starting point.

5. FIGURE OUT THE DIFFERENCE Once you've created your budget, keep records of your actual income and expenses. This keeps you aware of the difference between what you budget and actually spend.

BUILDING A BUDGET

This chart shows some rough guidelines on how much of your income should go toward different expenses. If you live in an area where transportation is higher than normal or rents/mortgage are higher, you may need to make adjustments. Also, if you would like to add a section for gifts, or something else, then you'll need to subtract from another area.

30%	HOUSING
18%	TRANSPORTATION
16%	FOOD
8%	MISCELLANEOUS
5%	CLOTHING
5%	MEDICAL
5%	RECREATION
5%	UTILITIES
4%	SAVINGS
4%	OTHER DEBTS

6. TRACK, TRIM AND TARGET Once you start tracking, you may be surprised to find you spend hundreds of dollars a month on eating out or other flexible expenses. Some of these are easily trimmed. Cutting back is usually a better place to start than completely cutting out. Be realistic. It will help you to be better prepared for unexpected costs.

The SMART Way to Trim Expenses

In finding ways to trim flexible expenses, it helps to have a goal to save toward each month. Setting such a goal needs to be SMART:

SPECIFIC Smart goals are specific enough to suggest action. Example: Save enough to visit Rome for your wedding anniversary. Not just "save money."

MEASURABLE You need to know when you achieved your goal or how close you are. Example: A trip to Italy costs $2,000, and you have $800 saved.

ATTAINABLE The steps toward reaching your goal need to be reasonable and possible. Example: I know I can save enough money each week to purchase that trip to Italy.

RELEVANT The goal needs to make sense. You don't want to work toward a goal that doesn't fit your need. Example: We would like to stay in four-star hotels in celebration of our anniversary.

TIME-RELATED Set a definite target date. Example: I want to go to Italy by next summer.

BUDGET WORKSHEET

Monthly Net Income	
Income #1	$
Income #2	$
Interest	$
Other	$
TOTAL INCOME	$

Monthly Flexible Expenses	
Food	$
Entertainment	$
Debt Payments	$
Other	$
TOTAL FLEXIBLE EXPENSES	$

Monthly Fixed Expenses	
Housing	$
Groceries	$
Utilities	$
Transportation	$
Health	$
Other	$
TOTAL FIXED EXPENSES	$

TOTAL EXPENSES	$

(add flexible and fixed expenses)

TOTAL MONTHLY INCOME	$
TOTAL MONTHLY EXPENSES	$
TOTAL FOR SAVING & INVESTING	$

WHERE TO TURN FOR HELP WITH DEBT MANAGEMENT

There's help available when you're in trouble. If you think you're falling seriously behind, credit counseling resources are available at little or no cost.

NATIONAL FOUNDATION FOR CREDIT COUNSELING
1.800.388.2227
www.nfcc.org

THE FEDERAL TRADE COMMISSION
http://www.consumer.ftc.gov

AMERICAN CONSUMER CREDIT COUNSELING
1.800.769.3571
www.consumercredit.com

Practical Money Skills for Life™

For more information, visit
www.practicalmoneyskills.com

PRACTICAL MONEY GUIDES

CREDIT CARD BASICS

What you need to know about managing your credit cards

Practical Money Skills for Life™

TAKE CHARGE WHEN YOU CHARGE

Credit cards can be powerful financial tools for you and your family, and as with all financial tools, they need to be used carefully. This guide outlines the basics of credit cards and the responsible use of credit.

PRACTICAL MONEY GUIDES

BUDGET BASICS
CREDIT HISTORY
CREDIT CARD BASICS
DEBIT CARD BASICS
PREPAID CARD BASICS
IDENTITY THEFT

When you understand how to manage your finances, you've got an invaluable tool in taking control of your life. Wise use of these skills can provide peace of mind, financial freedom, increased buying power and a secure future. This guide is one of a series on **PRACTICAL MONEY SKILLS FOR LIFE.**

THE CONVENIENCE OF CREDIT

Credit cards offer many features. There is the convenience of being able to buy needed items now and the security of not having to carry cash. You also receive fraud protection and in some cases rewards for making purchases.

With these advantages also come responsibilities. You need to manage credit cards wisely by understanding all of the card's terms and conditions; staying on top of payments; and realizing the true cost of purchases made with credit. Using a credit card is like taking out a loan. If you don't pay your card balance in full each month, you'll start paying interest on that loan.

Choose Wisely

The best way to maximize the benefits of credit cards is to understand your financial lifestyle – your money needs and wants. Once you determine how you'll use a credit card, it's important to understand all of the card's features including:

- Annual Percentage Rates (APRs) and whether rates are fixed or variable
- Annual, late and over-limit fees
- Credit limit on account
- Grace periods before interest begins accruing
- Rewards including airline miles or cash back

Stay Alert

Some credit card issuers offer free, personalized and automatic alert messages to your phone and email to help you keep track of:

- Available credit
- Balances
- Payment due dates
- Payment histories
- Purchase activity

Understand Your Rights

Credit cardholders are entitled to protections:

- Zero liability means you are not responsible for fraudulent charges when you report them promptly.
- In some cases, you have the right to dispute purchases with merchants for unsatisfactory products or services.

Follow the 20-10 Rule

This general "rule of thumb" helps you understand how much credit you can afford. Credit cards are loans, so avoid borrowing more than 20 percent of your annual net income on all of your loans (not including a mortgage). And payments on those loans shouldn't exceed 10 percent of your monthly net income.

Write it Out

Do you actually know how much debt you have? Many people don't. Start by making a list of everything you owe, whether it's a mortgage, a credit card or even student loans you took for the kids' education. Then write down:

- The lender name
- The amount you owe
- The term of the loan
- The interest rate and fees

Then total them up. The numbers will probably make you worry, but you've already made a positive step.

Think Three Years

Reducing debt is like losing weight. You're not going to lose 50 pounds in a month. You need realistic goals in reasonable timeframes. Same with debt. Most people take four to five years to become debt free. So aim for three years. It's not too long or too short.

Cut and Heal Spending

The best way to save money is to stop spending it. Cutting spending is the fastest way to reduce debt load. It's literally like a surgical "cut" of your finances. And once you start healing, you'll notice that your attitude, relations with others, emotions and sense of humor get better, too.

The True Cost of Credit Card Purchases

If you don't pay off your credit card balance every month, the interest assessed on your account means you may be paying more than you expect. See how much extra you might pay on a $1,000 credit card purchase with varying interest rates.

TOTAL PURCHASE AMOUNT The balance due on your credit card	$1,000	$1,000	$1,000
CREDIT CARD APR The annual interest rate on your credit card	10%	15%	25%
MONTHLY PAYMENT The minimum monthly payment	$40	$40	$40
NUMBER OF MONTHS TO PAY OFF PURCHASE AMOUNT* Time it will take to pay off the balance	29	31	36
TOTAL FINANCE CHARGE The total amount of money you will pay in interest alone	$126.02	$206.50	$427.22
TOTAL COST The final amount you will pay for your purchase	$1,126.02	$1,206.50	$1,427.22

* In general, this assumes that your account has no new charges and that your Annual Percentage Rate does not change. Paying more than the minimum will considerably shorten payoff times.

It's a good idea to check your credit reports at least once a year to see what they say about you. You can receive one free report per year from each credit bureau (listed on the back) by ordering them through www.annualcreditreport.com. (ADD LINK). Or, for a minimal charge, you can order additional copies from year bureau directly. Note: If you have been denied credit in the past 60 days, you have the legal right to receive another free copy of your report from the bureau that issued it.

CREDIT BUREAUS

EQUIFAX
Report Order: 1.800.685.1111
Fraud Hotline: 1.888.766.0008
www.equifax.com

EXPERIAN
Report Order: 1.888.397.3742
Fraud Hotline: 1.888.397.3742
www.experian.com

TRANS UNION
Report Order: 1.877.322.8228
Fraud Hotline: 1.800.680.7289
www.tuc.com

Practical Money Skills for Life™

VISA

For more information, visit
www.practicalmoneyskills.com

Practical Money Skills for Life™

PRACTICAL MONEY GUIDES

CREDIT HISTORY

Your credit history and how it affects your future

VISA

YOUR CREDIT HISTORY — THE RECORD OF HOW WELL YOU HANDLE CREDIT

To get a glimpse of your financial future, many businesses look at your financial past. This history is contained in your credit report. Your credit report determines everything from whether you qualify for a loan and the rate you'll pay on that loan, to renting an apartment and obtaining car insurance. This guide explains what credit bureaus are, why your credit history matters, and how to correct credit report errors and keep your credit rating strong.

PRACTICAL MONEY GUIDES

BUDGET BASICS
CREDIT HISTORY
CREDIT CARD BASICS
DEBIT CARD BASICS
PREPAID CARD BASICS
IDENTITY THEFT

When you understand how to manage your finances, you've got an invaluable tool in taking control of your life. Wise use of these skills can provide peace of mind, financial freedom, increased buying power and a secure future. This guide is one of a series on **PRACTICAL MONEY SKILLS FOR LIFE.**

What Is a Credit History?

Your credit history is a financial profile. It lets lenders, landlords and employers know how you have managed money in the past and helps them decide whether or not to do business with you. This history is contained in a credit report that is kept on file by the three independent credit bureaus listed on the back of this guide. It may include such information as:

- How promptly you have paid off credit cards and loans
- How well you have handled paying other bills, such as rent and utilities
- Your total outstanding debts
- How much available credit you have on credit cards and home equity loans

Who Can See Your Credit Report?

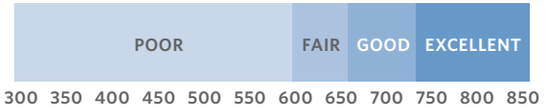
Your credit report can and most likely will be reviewed by anyone planning to give you a loan or credit, such as banks and credit unions, credit card issuers, auto financing companies, and insurance companies. Your report also may be checked by landlords and potential employers. Some lenders may also use the details in your report to determine how much credit they are willing to offer you and at what rate. Anyone with a legitimate business need can access your credit report, though an employer (or prospective employer) typically requires your written consent to do so.

Learn more about credit history and your FICO® credit scores at **www.whatsmyscore.org**.

Your Credit Score

When you apply for credit, lenders determine your credit risk by examining your credit scores (sometimes referred to as FICO® scores because they may be calculated using software developed by Fair Issac Corporation). Each of the three main credit bureaus – Equifax, Experian and TransUnion) – keeps credit information about you including your payment history, outstanding balances owed, length of credit history and number of recently opened accounts. They use that information to calculate your credit score.

FICO scores range from 300 to 850. The higher your score, the lower your perceived risk to the lender – and the more likely you are to receive more favorable credit terms.



To get a free estimate of your credit score, visit www.whatsmyscore.org/estimator.

How Your Credit Score Affects You

If you have a high credit score, you are more likely to be granted the credit you apply for. If you have a low credit score, you may be rejected or charged a higher rate of interest on credit you do receive. Charging higher interest rates is how banks make up for the increased risk that you may represent.

Raising your credit score can save you thousands of dollars in lower loan payments on your home, car and credit cards.

BEWARE OF "FAST FIXES" FOR ACCURATE CREDIT PROBLEMS

If you've had any late payments, foreclosures, or repossessions, this information stays in your credit report for up to seven years. If you've filed for bankruptcy, this information can stay in your report for up to 10 years.

Some companies claim they can "fix" such problems for a fee. However, it is legally impossible to alter an accurate credit history. If you find yourself in financial trouble, contact a member agency of the National Foundation for Credit Counseling (NFCC), the nation's largest national nonprofit credit counseling network, by calling 1-800-388-2227 or visiting **www.nfcc.org**.

Tips to Keep Your Credit Score Strong

- Complete credit applications carefully and accurately.
- Use your credit cards responsibly and don't let them reach their limit or spend beyond your means.
- Attempt to pay your credit card balance in full each month, but at least make the minimum payment by the due date.
- Know the dates your bills are due and always pay them on time.
- If you have problems paying your bills, contact your creditors. In many cases, they will work with you to figure out a payment plan.
- If you move, let your creditors know your new address as soon as possible to avoid losing bills or receiving them late.
- If your credit card is lost or stolen, report it immediately.
- Review your credit reports periodically for accuracy and report any errors immediately.
- Establish a consistent work history.

Checking Your Own Credit Report

It's a good idea to check your credit report at least once a year to see what it says about you. Just contact any of the credit bureaus listed on the back of this guide. You are allowed to see your credit reports for free every 12 months. However, if you have been denied credit in the past 60 days, you have the legal right to receive another free copy of your report from the bureau that issued it.

How to Correct Credit Report Errors

If your credit report contains any mistakes, credit bureaus are bound by law to correct them at no charge, providing that you inform the bureau of the problem in writing within 30 days of receiving your report. If the investigation of your claim does not yield a satisfactory result, you may send the bureau a written statement of up to 100 words to clarify. Be sure to include photocopies or other proof to support your claim. In many cases, the bureau will have to include your statement with any future reports that contain the disputed information.

If you know or suspect you are a victim of identity theft, contact the fraud department at one of the three main credit bureaus listed below. Request that they place a fraud alert on your file and contact the other two bureaus on your behalf.

You may also wish to contact the Federal Trade Commission's Identity Theft Hotline: 1.877.IDTHEFT (1.877.438.4338)

CREDIT BUREAUS

EQUIFAX
Report Order: 1.800.685.1111
Fraud Hotline: 1.888.766.0008
www.equifax.com

EXPERIAN
Report Order: 1.888.397.3742
Fraud Hotline: 1.888.397.3742
www.experian.com

TRANS UNION
Report Order: 1.877.322.8228
Fraud Hotline: 1.800.680.7289
www.tuc.com

Practical Money Skills for Life™

VISA

For more information, visit
www.practicalmoneyskills.com

Practical Money Skills for Life™

PRACTICAL MONEY GUIDES

IDENTITY THEFT

How to safeguard your identity and financial information from theft

VISA

PROTECT YOUR PERSONAL FINANCIAL INFORMATION TO AVOID CARD FRAUD AND IDENTITY THEFT

When your personal and financial information falls into the wrong hands, the consequences can be devastating. Identity thieves can use it to steal money from your accounts, open new credit cards and apply for loans, among other crimes. The information provided here can help you avoid becoming a victim and explain what to do if you know or suspect that your identity has been stolen.

PRACTICAL MONEY GUIDES

BUDGET BASICS
CREDIT HISTORY
CREDIT CARD BASICS
DEBIT CARD BASICS
PREPAID CARD BASICS
IDENTITY THEFT

Understanding how to manage your finances provides an invaluable tool to take control of your life. Wise use of these skills can provide peace of mind, financial freedom, increased buying power and a secure future. This guide is one of a series on **PRACTICAL MONEY SKILLS FOR LIFE.**

WHAT TO DO IF YOUR IDENTITY IS STOLEN

If you suspect you have been, or are about to be, a victim of identity theft, it is important to act quickly. Contacting the proper agencies and filing the necessary reports will go a long way toward minimizing damage to your financial well-being.

CREDIT BUREAUS Immediately contact the fraud department at one of the three main credit bureaus listed on the back of this guide and ask that they place a 90-day initial fraud alert on your credit file. Whichever bureau you contact will notify the other two to do the same. You'll be entitled to one free credit report from each bureau.

You can also request a security freeze, which prevents credit issuers from obtaining access to your credit files without your permission. This can help prevent thieves from opening up new credit cards or other loans in your name. There may be a fee associated with placing a security freeze on your credit files.

LAW ENFORCEMENT File a detailed identity theft report with the police department. Search the Federal Trade Commission's website (www.consumer.ftc.gov) for instructions on how to create and file a report. You'll also need to send copies of the report – by certified mail, return receipt requested – to the credit bureaus and companies whose accounts were impacted.

FEDERAL TRADE COMMISSION (FTC) Although the FTC doesn't investigate individual identity theft cases, if you file a complaint they will share the information with an online database shared by thousands of civil and criminal law enforcement authorities, worldwide.

CREDIT CARD ISSUERS AND BANKS Contact the credit card issuer, which will closely monitor your account for odd behavior. They may either reissue a card with a new CVV (card verification code) number or issue an entirely new card number. Close affected bank accounts and obtain new ones. If checks were stolen, ask the bank to stop payments. Also, change any related passwords or PIN numbers and notify companies that have automatic payments tied to the account to make sure you don't miss a payment.

Six Ways to Protect Yourself

There are several simple steps you can take to reduce or minimize the risk of becoming a victim of identity theft or card fraud.

PRACTICE SAFE INTERNET USE Delete spam emails that ask for personal information, and keep your anti-virus and anti-spyware software up-to-date. Shop online only with secure web pages (look for "https" in the address bar and check for an image of a lock). Never send credit or debit card numbers, Social Security numbers and other personal information via email.

DESTROY PERSONAL FINANCIAL RECORDS Once they're no longer needed, shred credit card statements, ATM, credit/debit card/deposit receipts, loan solicitations and other documents that contain personal financial information.

SECURE YOUR MAIL Empty your mailbox quickly and get a mailbox lock. When mailing bill payments, checks and other sensitive documents, consider dropping them off at the post office or a secure mailbox.

GUARD YOUR SOCIAL SECURITY NUMBER Thieves seek your Social Security number because it can help them access your credit and open bogus accounts. Never carry your card; instead, memorize your number and store the card securely. Don't have your number printed on checks and ask your employer to remove it from pay stubs and other correspondence.

CHECK YOUR CREDIT REPORTS Regularly review your credit reports for suspicious activity. You can request one free copy of each report per year at www.annualcreditreport.com; otherwise contact the three credit bureaus directly (Note: They'll charge a small fee).

BEWARE OF SCAMS Always be on the defensive with your financial information. Never give out personal information to telemarketers or via email from someone claiming to represent your bank, credit card issuer, a government agency, a charity, or other organization unless you initiated the contact. If you think the request is legitimate, contact the agency directly to confirm their claims.

Protect Your Children's Identities

Identity thieves are increasingly targeting children's identities, using their Social Security numbers to illegally obtain jobs, credit accounts, mortgages and car loans. Use the same precautions handling their personal information as with your own, and if you suspect identity theft, follow the same theft report procedures.

Tips For Frequent Travelers

Whether you're traveling for business or pleasure, be on the alert for opportunities that thieves may try to take advantage of:

- Receipts—Don't leave credit card receipts on restaurant tables; sign and hand them directly to the server. Keep your copy of all receipts.
- Wallets—Stolen wallets frequently lead to identity theft, so instead of carrying your wallet in your pocket or bag, consider using a travel pouch worn under your clothing.
- Checks—Leave your checkbook at home, safely stored.
- Camera phones—That tourist with a camera phone may actually be shooting your credit card or driver's license. Keep important personal information out of view from others.
- Mail—Put a delivery hold on your mail whenever you travel.
- Hotels—Lock up all valuables in room or hotel safes while you are out, including laptops, passports and other documents containing personal identifying information. Don't leave these items with a hotel doorman to transport or hold—carry them yourself.
- Airplanes—Don't put any items that contain your Social Security number, card or account numbers in checked luggage. Always carry those items in carry-on luggage.

HOW TO PROTECT YOURSELF AND YOUR MONEY

Once you've chosen a prepaid card or received one, it's up to you to keep your money safe. Here's how:

USE THE CARD CAREFULLY Keep track of your balance so you don't get charged a fee for trying to spend more than is available. If your wages or other benefits are deposited directly onto the card, make sure you know the amount of the deposit and when it will happen.

KEEP YOUR PIN SECRET Pick a number that's hard for someone else to guess – not your birthday or address. Don't tell it to anyone or write it anywhere it could be easily found.

GET THE IMPORTANT INFO Make sure you know your card issuer's policies for lost or stolen cards, and keep your card number and the customer service phone number in a safe place at home.

ACT QUICKLY If your card is lost or stolen, let the card issuer know right away. Most card issuers will freeze the funds so the card can't be used and send you a new card with your remaining balance on it.

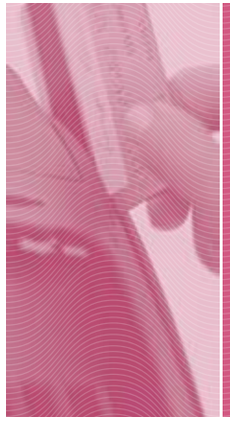
Practical Money Skills for Life™

VISA

For more information, visit
www.practicalmoneyskills.com

VPMSFL10INSRTPB

Practical Money Skills for Life™



PRACTICAL MONEY GUIDES

PREPAID CARD BASICS

What you should know about using prepaid cards

VISA

PREPAID CARDS — AN ALTERNATIVE TO CASH

A prepaid card is a card you load with money to make purchases anywhere a debit card is accepted. It's a safe alternative to carrying cash and paying check-cashing fees. In lieu of travelers checks, prepaid cards can be good options for traveling. They're also a popular gift-giving idea because recipients can use them for whatever they want, and they're widely accepted.

PRACTICAL MONEY GUIDES

BUDGET BASICS
CREDIT HISTORY
CREDIT CARD BASICS
DEBIT CARD BASICS
PREPAID CARD BASICS
IDENTITY THEFT

When you understand how to manage your finances, you've got an invaluable tool in taking control of your life. Wise use of these skills can provide peace of mind, financial freedom, increased buying power and a secure future. This guide is one of a series on **PRACTICAL MONEY SKILLS FOR LIFE.**

What Are Prepaid Cards?

A prepaid card looks like a debit or credit card and similarly allows you to make purchases without cash or checks. Unlike credit cards, you cannot take on debt with a prepaid card, nor are prepaid cards linked to your bank account like debit cards.

A prepaid card has a zero balance until money is added to it. When you make a purchase with a prepaid card, the amount is subtracted from the balance on the card. Once the balance reaches zero, the card is empty. Some prepaid cards can have money reloaded on to them so they can continue to be used. Others, such as gift cards, can be discarded when all of the funds are spent.

With Prepaid Cards You Can:

- Make purchases in person, online, or by phone
- Give gifts to friends and family
- Withdraw cash from an ATM or bank
- Receive wages or funds by direct deposit to the card
- Pay bills

HOW DO PREPAID CARDS WORK?

When you use a prepaid card to make a purchase, the amount is subtracted from the balance of the card. Once the balance reaches zero, the card can be thrown away unless it is a reloadable card, in which case you can add funds and continue using it.

Many employers and government agencies use prepaid cards instead of checks to deliver wages, child support, unemployment, and other benefits.

Choosing a Prepaid Card

When choosing a prepaid card that is right for you, consider the following questions:

- Ask if you can put money on the card yourself, how to do that, and what it costs.
- Get information about where and how you can use the card.
- Find out if your prepaid card comes with monthly statements and how you can check the balance over the phone or online.
- Understand all associated fees for services like activation, monthly maintenance, balance reloading and fees to receive paper statements.

Kinds of Prepaid Cards

OPEN LOOP VS. CLOSED LOOP The two main types of prepaid cards are open loop and closed loop cards. Closed loop cards are merchant-specific, used for transactions exclusively at a particular merchant's locations. An open loop card is associated with and bears the logo of an electronic payment network, such as Visa; open loop cards are honored wherever these networks are accepted.

RELOADABLE CARDS A reloadable prepaid card is one that lets you add funds after your initial purchase. Teen cards, travel cards, and payroll cards are often reloadable.

GIFT CARDS These non-reloadable prepaid cards can be given as gifts and used until the balance is zero.

TEEN CARDS Parents can teach teens financial responsibility while monitoring their spending with teen cards.

TRAVEL CARDS Travel cards are an alternative to cash and travelers checks while traveling. Some cards offer lost luggage reimbursement, emergency card replacement, and zero liability for lost or stolen cards.

PAYROLL CARDS A payroll card is an alternative to traditional payroll methods in which an employee's wages are deposited directly to his or her card.

HEALTHCARE CARDS Healthcare cards are a specific type of prepaid card that let you access funds you've set aside in an employer-provided Flexible Spending Account or a Health Savings Account tied to a high-deductible health insurance plan. You can use the card as you would a debit or credit card to pay for qualified medical expenses such as doctor's visit copayments, prescription drugs and over-the-counter medications purchased with a doctor's prescription.

Features to Look For In a Prepaid Card

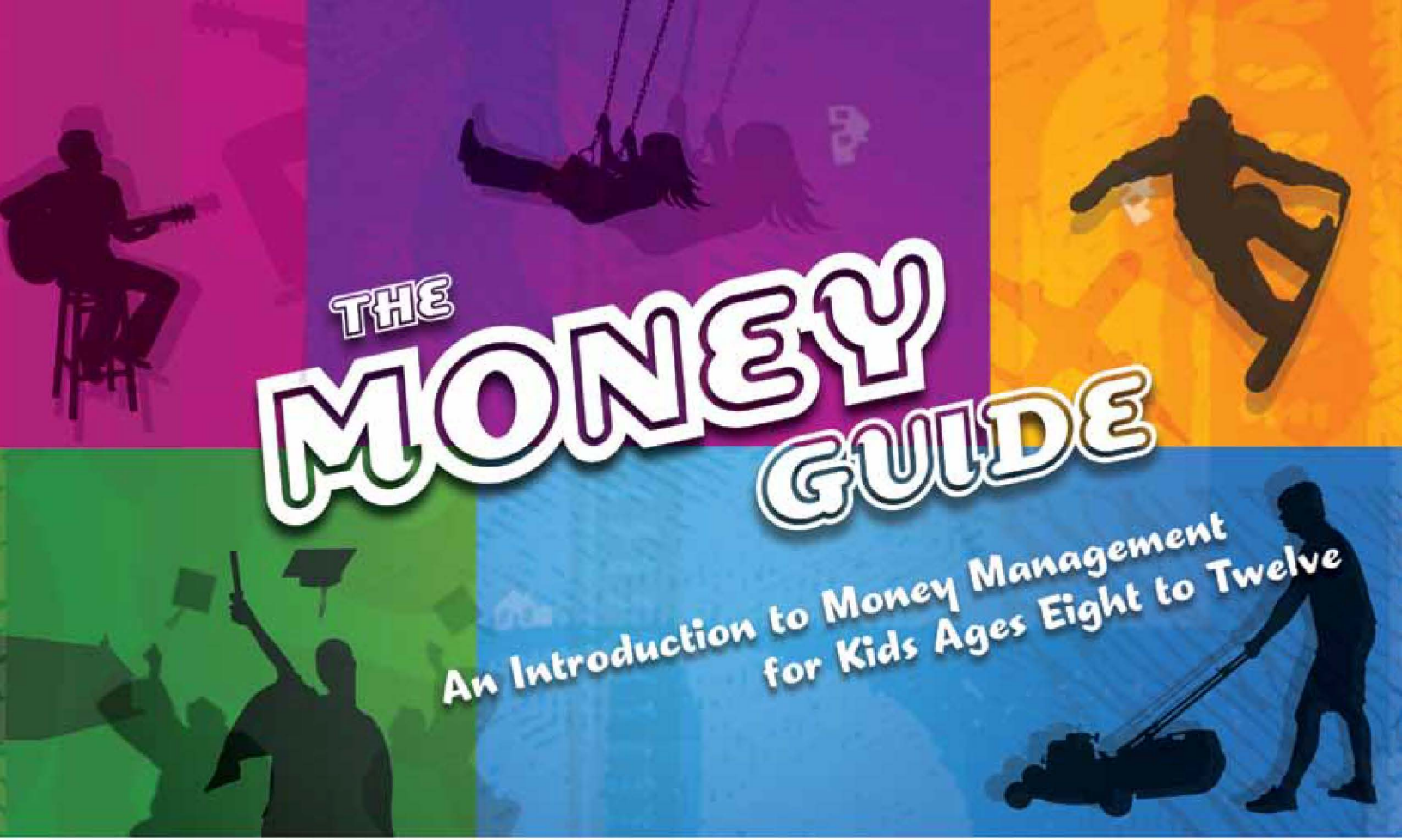
There are many prepaid cards out there, and choosing the right one is important. What features are most important to you?

RELOADABLE Some prepaid cards allow you to add money once the balance reaches zero. Gift cards are not reloadable.

LIABILITY PROTECTION Some prepaid cards will protect your balance in case the card is lost or stolen. Look for a card that offers a Zero Liability policy.

EXPIRATION DATES While many cards do not expire, some do carry monthly maintenance fees, which can reduce your card balance. Prepaid cards are best for storing money you intend to spend in the short term.

LOW FEES Is there an activation fee charged when you set up the card? What are the fees charged for ATM withdrawals? Take note of any fees associated with the card you choose.



Practical Money Skills for Life™

VISA

Game or bike?
Movie or shoes?
Chocolate sundae with extra rainbow sprinkles on top?

One of the best things about having your own money is that you get to decide how to spend it. Whether you get a weekly allowance, receive birthday cash or gift cards, or find a quarter on the street, your first task to handling your money well is to think about short-term and long-term goals. Then make a plan to reach them!

It takes a bit of practice to become great with money, just like it took a little practice to learn to ride a bike. But once you get the hang of it, you'll be ready to tackle all sorts of money twists and turns.

Race ya to the bank!

How to Be Awesome with Your MONEY

THE GOAL

of an allowance is to learn to manage money wisely. The amount of your allowance should be based on what you need, not how you behave.

Kids listen up!

(You already behave right ... right?)

Allowances are different for every family. Your goal is to learn to manage any amount of money, big or small. Older kids usually get more allowance than younger kids. Don't worry, you'll be older soon!

Parents take charge!

Allowance is easy to figure out. Track your kids' discretionary expenses (toys, mobile devices, candy) and non-discretionary expenses (school lunches, clothes). Decide which expenses you want them to manage. Set a reasonable amount for each category. Increase allowance as your child becomes more confident. Don't worry if they make mistakes. That's part of the learning process!

How does your allowance compare to what your parents got when they were kids? Find out at www.practicalmoneyskills.com/allowance.

ASK ANDREW

Q: Can I get an allowance for doing chores?
A: Nope! Do them anyway.
Q: Being nice to my brother = allowance?
A: Not! Try kindness every day.

Who pays? You pay! It's YOUR allowance:

- Candy
- Music downloads
- Mobile phone
- MP3 player
- Movies
- Video games
- Birthday gifts
- Baseball cards

EARNING

You've gotta make it before you spend it!

The world is your CLASSROOM

—sit anywhere you'd like.

Fast Fact

Although the average cost of college tuition and fees is $46,000 over four years, having your college degree may greatly increase your earning potential.

Over a lifetime of work, college grads earn about $1 million more than high school grads!

Hurry, don't be late for class!

Okay, so right now you may be stuck in the third row for geography class. But here's a top-secret tip about learning: getting an education is like getting an all-access fun pass. The more you learn, the more things you can do and the more places you can go.

How 'bout volunteering?

A volunteer position is a great way to learn about teamwork, leadership and real-life job skills. Local animal shelters, retirement homes and parks and recreation departments are often looking for volunteers. Look online or ask about volunteer opportunities at organizations in your neighborhood.

Get up-to-date info on banking, financial aid, student loans — even back-to-school budgeting. Check out www.practicalmoneyskills.com.

Pizza?
Or Pizza AND a movie?
You need a budget!

Let's say your allowance is $20 this week. You go to the movies on Monday and spend it all (oops!). On Saturday your friends want to get pizza. But you're out of cash!

If you had followed **a budget,** you could have planned for two activities during the week: $10 x 2 = $20. Now what? Sell some of your favorite video games to friends?

Budgets are really helpful when you need to save up for something. For example, you want a new digital camera for summer vacation. A budget will help you focus on how much to save and for how long. Waiting to buy can work in your favor. That digital camera you've had your eye on? It could go on sale and cost way less in just a few months' time.

YOUR PENNIES ARE LIKE A PIZZA.

Break down your spending like that pie!

Senator, is that pepperoni I smell?

$PENDING

Stuff you need vs. stuff you want.

Play free money games and puzzles. Check them out by visiting www.practicalmoneyskills.com and clicking on Games.

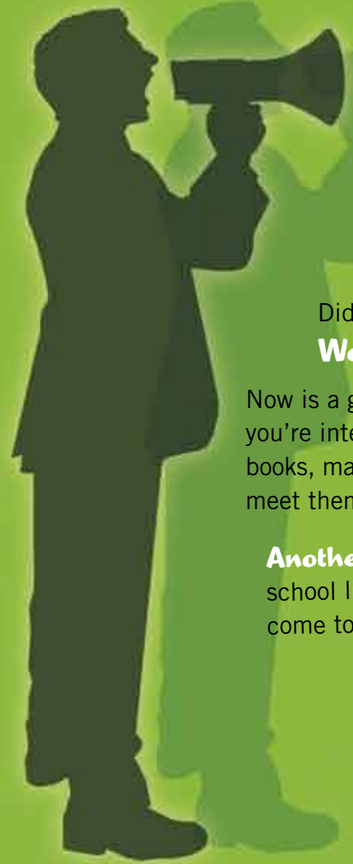
WHAT CAREERS INTEREST YOU?

Consider these when choosing:

- Work environment
- Job demands
- Training and education
- Salary range
- Travel
- And fun!

You are the BOSS of your own life.

Hey, isn't that a Tyria Jacobaeae?



Pastry Chef?
Bug Catcher?
Rocket Scientist?
Video Game Programmer?

Did you know the average person holds 10 or more jobs during a lifetime? **Wow!** That means you can be lots of different things when you grow up.

Now is a great time to start exploring jobs. Don't be afraid to check out things you're interested in — even if they seem out of reach. How? Read about jobs in books, magazines or online. Your parents know someone with a cool job. Ask to meet them and see where they work and what they do each day.

Another good way to explore jobs is to join a career club. Ask your school librarian if there's a career club in your area. All sorts of people come to career club meetings to explain what they do at their jobs.

All work and no play? Take a break and try playing Financial Football online. Head to www.practicalmoneyskills.com/football.

The key to saving success?

Get in the habit of doing it regularly!

Start saving early, and often. Some portion of the money you earn should be set aside for short-term savings, like funds for purchasing toys or games; and long-term savings, such as a college fund.

How do you make saving more exciting? Ask your parents to set up a matching plan when you open a savings account at the bank. For example, if you save $5, your parents add $5, for a total of $10. Watching your dollars add up quickly is a good incentive to keep saving.

Save money in a bank
Ten cents is a dime.
Move a clock forward or back
That's daylight savings time.

Now if you'll excuse me, I must attend to my wooden teeth.

Going up?

THE POWER OF COMPOUND INTEREST

Save this each week	At % Interest	In 10 years you'll have
$7.00	3%	$4,298
$14.00	3%	$8,596
$21.00	3%	$12,894
$28.00	3%	$17,192

A working budget is key to a solid financial plan. Visit www.practicalmoneyskills.com/savingforagoal and use this calculator to see how much and how often you need to start saving to meet your goal.

SAVING

The long and short of it.

Someday I'll live in a

BIG OLE HOUSE

with a horse in the back yard!

Livin' Solo Learn some of the money skills you'll need to make it on your own someday by playing our free Financial Soccer video game at www.practicalmoneyskills.com/soccer. Parents and teachers can check out our lesson plans, too at www.practicalmoneyskills.com/lessonplans.

What? No parents?

Eat whatever I want?

Put my feet all over the furniture?

Yep, someday you're going to live on your own and get to make all the decisions. House or apartment? City or country? Dog or cat?

Maybe you'll decide to get married, have kids or start your own business. Those are all great goals that can enrich your life, but they're costly too. You'll need all the money skills you can to succeed. Welcome to responsibility.

Millionaire?
Gazillionaire?

How are you going to get there?

Everyone wants to have plenty of money and the freedom to spend it however they choose. You can do it! It takes hard work and clever strategies — like making your money work even harder than you do.

The longer your money stays in the bank, the more money it will earn for you. The money earned is called interest. The higher the interest rate, the more money you earn. See how hard you can make your money work!

After the first year, you will start to earn interest on your interest. That means in the second year and after that, these numbers will be even higher!

What will your $20 bucks be after one year?

Interest	Total
3%	$20.60
5%	$21.00
7%	$21.40

Example:

One year at 5% interest:

$20.00
x .05
1.00
x 1 year
=$1.00

So 20.00 + 1.00 = $21.00

How long before I become a MILLIONAIRE?

Hint: Use the Save a Million Calculator! Go to www.practicalmoneyskills.com/saveamillion.

Remember, money doesn't grow on trees. But it does grow in the bank!

Stop dreaming about all that money and start saving now!

Car? College? Cabin by the lake?

Sometimes you may need to borrow money from a bank to purchase an expensive item. Like a car, for example. Well, unless you have a lot saved up, you'll probably need a loan. The bank will lend you the money and you will pay it back with interest. Which means the dollar amount you borrowed plus a little extra for the favor.

When you use a loan to buy something, it's important to think of the cost of what you're borrowing. For example, let's say you find there is a sale on the MP3 player you've been dying to get. If you buy that MP3 player on credit and don't pay off the loan right away, the interest you will owe could wind up costing you far more than the money you saved from the sale.

Be careful! Always look at the TRUE cost of an item first!

For the true cost of credit card purchases,
use this simple calculator at www.practicalmoneyskills.com/costofcredit.

BORROWING

Big dreams with big price tags.

Just remember —

PRACTICE EVERYTHING YOU'VE LEARNED!

Whether it's budgeting, saving or spending,
the more you do it, the better you'll get.

One more thing:

Gaining confidence about money handling isn't all about math. It's about understanding good money habits and setting goals. Review this guide frequently when practicing and show it to your friends. Who wouldn't want to be great with money?

Have You Mastered Your Money?
You can sharpen your skills and teach your parents a thing or two at www.practicalmoneyskills.com.

Good luck — you can do it!
Just take it easy at the mall, okay?

CONGRATULATIONS!

You're well on your way to becoming awesome with money.

Practical Money Skills for Life

Visa Inc.'s Practical Money Skills for Life is a free, award-winning program designed to help teachers, parents and students improve their money management skills. The program features financial education tools and resources, including games, planners, calculators, lesson plans, worksheets, quizzes, podcasts and brochures.

Visa has worked with leading educators, consumer advocates and financial institutions for over a decade to promote financial education throughout America. Millions of students have learned the fundamentals of personal finance through the Practical Money Skills for Life program.

Visit www.practicalmoneyskills.com to take advantage of these valuable resources.

Practical Money Skills for Life™

To learn more about Practical Money Skills for Life, visit www.practicalmoneyskills.com.

VKIDSMONEYGUIDE 01.11

VISA

FOR MORE INFORMATION VISIT:

whatsmyscore.org

whatsmyscore.org

MONEY101

PRESENTER'S GUIDE

A CRASH COURSE IN
BETTER MONEY MANAGEMENT
FOR COLLEGE STUDENTS

VISA

DEAR PRESENTER,

It's well known that many students lack basic money management skills. They're in a new environment, possibly away from home for the first time, and most aren't prepared for the financial responsibility that comes with student loans, credit card offers, lease signings and more. And the stakes are high – bad decisions today can have serious consequences for years to come.

Research shows financial literacy programs work and early intervention education offers outstanding benefits. Students who learned about personal finances before they received a credit card had dramatically more responsible behavior than students who had no education. Those students who went through a program similar to the one you hold in your hands had 42% fewer late fees on their credit cards and had revolving balances that were 26% lower.

Visa is committed to helping young adults learn the fundamentals about wise money management. That's why we've introduced this Student Money Guide 101, aimed at college students and other young adults. What's My Score Student Money Guide 101 joins the What's My Score website (www.whatsmyscore.org) and Practical Money Skills program (www.practicalmoneyskills.com) as core pieces of Visa's effort for over 15 years to raise Americans' financial literacy using effective, compelling and relevant educational resources.

Together, we can help teach young adults the basics of sound financial skills that will last a lifetime.

Sincerely,

Nathaniel Sillin
Head of Global Financial Literacy,
Visa Inc.
nsillin@visa.com

USING THIS CD-ROM: Insert the CD and press the "Start Presentation" button. You can use the icons in the lower left of the screen to jump between sections easily. Use the forward and back button on the bottom right to move forward or back within each section.

GETTING STARTED

THE CD-ROM CONTAINS A MULTIMEDIA FLASH PRESENTATION THAT CAN ALSO BE PRINTED AS A PDF. IT FEATURES SIX TOPICS THAT SHOULD TAKE APPROXIMATELY 20 MINUTES EACH, DEPENDING ON DISCUSSION. IF YOU HAVE LIMITED TIME, WE RECOMMEND THAT YOU COVER THE INTRODUCTION, BUDGETING, ONLINE BANKING AND UNDERSTANDING CREDIT SECTIONS.

› **PRESENTATION:** Many of the concepts dealt with here are abstract, especially to young adults. Obviously, it's important to use humor and real world examples in order to make the subject matter relevant to your students. We encourage you to use the What's My Score Money 101 Student Workbook as a jumping off point and to engage your students in ways that no CD-ROM, workbook or computer can.

› **PRESENTER'S GUIDELINES AND SUGGESTIONS:** The What's My Score Money 101 curriculum is designed to help you begin the process of teaching young people the importance of financial responsibility. What follows is a lesson-by-lesson breakdown of the presentation and of the thinking that went into its development. We encourage you to use this general outline as background information to help you flesh out your own presentation. Think of it as talking points, not as a script.

› **STUDENT WORKBOOK:** The Money 101 Student Workbook is available through our website, www.whatsmyscore.org, as a printable download. Prior to beginning your presentation, hand out this student workbook with activities on each of the topics. Take advantage of some selected websites for student reference, which are included on the back page of the workbook.

› **ADDITIONAL OPPORTUNITIES:** Work with the campus newspaper or local media to promote a money management campaign for students. Hold an informal seminar or a questions and answers session. Find a student who might be willing to talk about bad financial decisions that he or she has made – and the consequences of those decisions.

› **ADDITIONAL MATERIALS:** For additional free financial literacy materials visit our orders page at whatsmyscore.org/orders. There you will find teaching materials, games and content all geared to educating consumers about the importance of financial literacy.

BUDGETING YOUR MONEY

WE START THIS PRESENTATION WITH BUDGETING YOUR MONEY BECAUSE UNLESS STUDENTS KNOW WHAT THEY HAVE AND WHERE IT'S GOING, THE REST OF THIS PRESENTATION DOESN'T AMOUNT TO MUCH. THE JUMPING OFF POINT IS TRACKING EXPENSES AND LOOKING AT SPENDING PATTERNS. FROM THERE WE GET INTO MAKING A PLAN AND KEEPING A BUDGET.

› **A1: OVERVIEW**
The key to understanding personal finances is being aware of expenses and income. Students need to track where their money is going and how much money is coming in each month. After getting a snapshot of their spending habits, students can get to work on their own personal budgets.

› **A2: TRACKING EXPENSES**
Students need to save all receipts and track every expense for a month. It's a real eye-opener to see where the money goes. Point out how much money goes towards small purchases, like daily coffee.

› **A3: WHY BUDGET?**
What is a budget and why is it important? What are the consequences of not keeping a budget?

› **A4: BUDGETING IDEAS**
Here are some simple ways to help stay on top of a budget. Invite students to offer other ideas.

› **A5: MAKING A PLAN**
After tracking expenses for a month, students should have an idea of where their money is going. Now it's time to put a monthly budget down on paper.

› **A6: BUDGETING TO MEET PERSONAL GOALS**
Now students can learn how to budget to meet goals, both long- and short-term, by adjusting their budgets each month.

DEBIT CARDS

A DEBIT CARD IS AN ATM CARD BUT AN ATM CARD ISN'T NECESSARILY A DEBIT CARD. GET IT? THE DIFFERENCE IS THAT A DEBIT CARD WILL HAVE A VISA LOGO ON IT AND CAN DO SOME THINGS THAT AN ATM CARD CAN'T. IN THIS SECTION WE'LL GO INTO THE DIFFERENCES AND THINGS TO LOOK OUT FOR WHEN USING A DEBIT CARD. IT MAY LOOK JUST LIKE A CREDIT CARD BUT THERE ARE IMPORTANT DIFFERENCES.

› **F1: OVERVIEW**
It's important to remember that although a debit card looks a lot like a credit card, there are some key differences to keep in mind.

Cash in/cash out. Every debit card transaction is linked directly to the checking account and is only good for the amount currently available. It is not a credit card.

› **F2: THE DEBIT CARD**
A debit card is only as good as the checking account that's behind it. For that reason, it's a more prudent choice for some college students – less credit, less temptation. Like a credit card, it's nearly universally accepted and is as good as cash.

› **F3: WHEN TO USE A DEBIT CARD**
Debit cards are best used for things like groceries, gas, restaurants or movies. When you need cash but are not near an ATM, many retailers offer cash back after purchase.

› **F4: CARD SECURITY**
Security is of utmost importance when it comes to debit cards. It's important to remember basic security tips around protecting PIN numbers, like covering the keypad when making transactions and never sharing the PIN with anyone.

Keep receipts. Although only some account numbers show on the receipt, it's never a good idea to leave important documents lying around.

› **F5: KNOW THE DIFFERENCE**
Look for the Visa symbol to identify a debit card. ATM cards do NOT have a Visa logo and can only be used at bank ATMs (Automatic Teller Machines) or authorized ATM affiliates listed on the back of the card.

Take control of your credit score

A guide to understanding and improving your credit.

WHATSMYSCORE.ORG

VISA

What is a credit score?

Your credit score is a number between 300 and 850, assigned to you by a credit bureau, that helps lenders decide how creditworthy you are — the higher the score, the lower the risk. Because credit can affect many important aspects of your life, getting and keeping your score as high as possible is vitally important. Armed with the following information, boosting this important number will be easier than you may think.

How is your score determined?

The most common used scoring system for credit scores is developed by FICO™ bureaus use this formula to evaluate how much risk you pose to potential lenders, based on the following factors:

35%
Payment history
Do you pay bills on time? Any recent missed payments?

30%
What you owe
Your debt balance as well as the ratio of your debt to your credit limit is an important factor in determining your score.

15%
Types of credit
Which credit cards you use and loans you carry also play a role in your credit score.

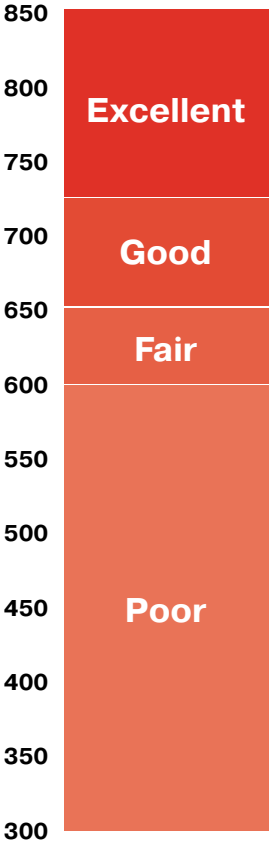
10%
New accounts
Opening many new accounts in a short period of time can negatively affect your score.

10%
Length of credit history
How long you've had credit will factor in to your final score.

Credit scores are based on your financial behavior and history, and do not include factors such as gender, race, religion, national origin, gender, age, education level or marital status.

What is a good score?

There is no absolute standard that lenders use to approve or deny credit. The chart below is merely a guide. Remember, a good score is one that works with, not against, your life goals. Staying informed and making smart financial choices is your best strategy for keeping your score on a steady climb.



Why a good score matters.

The reasons to keep your credit score in good shape are numerous.

House or apartment hunting. Whether you are renting or buy your first home, both landlords and mortgage lenders will require a good credit score.

Job Opportunities. Prospective employers often review candidates' credit history as a gauge of character and responsibility.

Better interest and insurance rates. A high score often qualifies you for lower rates on loans, and better deals on insurance.

Financial flexibility. A good credit score leaves the door open for additional credit, should you need it down the road.

How to improve your score.

If your score isn't exactly where you want it to be, all is not lost. Your credit score is very fluid and by taking action now, you can help improve your score quickly and keep it higher in the long run.

Always pay monthly bills on time.

Late payments can stay on your credit report and slow down your ability to improve your score.

Get credit. Use it.

Using credit is the only way to build credit history. If you don't currently have any credit accounts, open one and use it wisely.

Don't max out your cards.

Don't be tempted to spend up to your credit limit. If your debt is more than 25% of your total credit limit, your credit score may begin to fall.

Don't be afraid to talk to your creditors.

Lenders may be able to modify your interest rate or lower your monthly payment. But not if you don't ask.

Avoid opening new accounts to spread debt around.

Opening new accounts, especially in a short period of time, can negatively affect your score.

Monitor your credit regularly.

You aren't penalized for checking your own credit report. Check it for errors and potential fraud on a regular basis.

800

It's your credit. Don't neglect it.

While your credit score gauges your creditworthiness with a number, your credit report tells the full story of your financial activities. Every year, or more frequently if you suspect fraud or errors, check your report. You are entitled to a free copy annually from any of the three main credit bureaus.

Equifax	Experian	Trans Union
Credit Reports:	**Credit Reports:**	**Credit Reports:**
1.800.685.1111	1.888.397.3742	1.877.322.8228
Fraud Hotline:	**Fraud Hotline:**	**Fraud Hotline:**
1.888.766.0008	1.888.397.3742	1.800.680.7289
www.equifax.com	www.experian.com	www.tuc.com

You can also get a free credit report at www.AnnualCreditReport.com

Get a free credit score estimate now.

Our FREE credit score estimator is a great tool for keeping an eye on your score. Simply answer 10 questions and get an accurate estimate of your score. No personal data or log in process is required. Then make a pact with yourself to raise your score, and check it again in a year's time. By simply making smart financial choices, your score should begin to improve.

Visit www.whatsmyscore.org/estimator to try our free credit score estimator.

Today's date:

Today's credit score estimate:

- ☐ I will pay my monthly bills on time.
- ☐ I will use credit responsibly.
- ☐ I will pay more than the minimum due.
- ☐ I will contact my creditors if I can't pay a bill.
- ☐ I will check my credit report regularly.

Check your score a year from today:

Be sure to take advantage of all of the resources for controlling your personal finances at **www.whatsmyscore.org**

WHATSMYSCORE.ORG

VISA

VWMSCREDSCORE 0110

Research the institution's policies. For example, what does its privacy policy say about how it will use your personal information? Does it offer a "zero liability" guarantee for any unauthorized transactions? Will it reimburse any late fees if your bill payment isn't sent as scheduled?

Create a strong password for your account. The longer the password, the harder it is for someone to figure out, especially if you use a combination of capital and lowercase letters, numbers and symbols. Don't make a password out of a pet's name, birthdate, or other personal information.

Keep your ID/username and password private. Don't share it with anyone and don't leave it where someone could find it. Change your password regularly; change it immediately if you think it has been compromised. Don't allow your browser to "Remember my password" or "Remember me on this computer" for financial accounts.

Log off the banking website when you are done with your session or if you have to step away from the computer, and close the browser window after signing off. On shared computers, clear your "cached" activity by clicking on the "Tools" menu (in most browsers) and selecting "Clear Recent History" or something similar. (The words may be slightly different depending on the browser you use.)

Password-protect your home wireless network so that strangers can't access your wireless Internet account and possibly capture the data you send and receive. Call your Internet service provider for instructions on how to do this.

Use a firewall, which is a virtual barrier between your computer and the Internet. Your computer's operating system (OS) may have a built-in firewall; make sure it's turned on. Update your antivirus and antispyware software to guard against new malware as it appears. (Some banks offer customers free or reduced-price virus protection software.)

Avoid online banking when using public or unencrypted wireless networks (Wi-Fi). If you must use public Wi-Fi, take precautions. Look for the closed padlock or unbroken key in the browser frame and an "s" after "http" (http**s**://) in the Web address, which indicates an SSL (Secure Sockets Layer) connection.

> ***Phishing emails*** are fraudulent messages that try to get you to reveal sensitive information by making you believe you are communicating with a legitimate business. Often, these messages include a link to a copycat website, which is designed to look authentic and lure you into revealing your personal information. And remember, your bank will never contact you and ask for your Social Security number or password via email or phone.

Don't send sensitive information via email, chat or instant messaging (IM).

Know how much time it takes your bank to get a payment to your creditors after receiving your online bill payment request. Some payments, typically to larger creditors, are made electronically and may reach their destination within a couple of days of your request. Payments to smaller creditors, such as your dentist, may take a week or more because the bank sends an actual check to the recipient. Leave plenty of time for payments to reach your creditors before the due date.

Monitor your account activity regularly—even daily. In most cases, you must report unauthorized account activity to the bank within a certain time period (say, within 60 days of when the transaction first appeared on your statement) for full protection. If you don't, you may not be reimbursed for fraudulent transactions.

Check your monthly statements every month, even if you fail to get an email reminder. Place a reminder on your calendar of when to check for a new statement each month.

Assistance and information

If you are already a customer, you can contact the financial institution's customer service department for help with online banking. The following resources may be helpful when considering a new financial institution or to learn more about staying safe online.

Federal Deposit Insurance Corporation (FDIC)
www.fdic.gov / 877-275-3342

Contact the FDIC to confirm that any bank you are considering doing business with is insured.

National Credit Union Administration (NCUA)
www.ncua.gov / 800-755-1030

The NCUA administers the National Credit Union Share Insurance Fund (NCUSIF), which provides deposit insurance for credit unions much like the FDIC does for banks. Visit the NCUA site or call to find out if the credit union you're considering joining is insured.

OnGuard Online
www.onguardonline.gov

The U.S. federal government and the technology industry provide information and tips to promote online safety and security.

Privacy Rights Clearinghouse
www.privacyrights.org

The nonprofit Privacy Rights Clearinghouse offers a library of information, from tips for protecting your privacy online to how to shop safely on the Internet.

Consumer Action

www.consumer-action.org

Consumer advice and referral hotline:
hotline@consumer-action.org or 415-777-9635
Chinese, English and Spanish spoken

Consumer Action created the Digital Dollar series with funding from Visa Inc.

VISA

consumer action
Education and advocacy since 1971

Visit Visa's financial education program, Practical Money Skills, at: ***www.practicalmoneyskills.com***

Your Digital Dollars

Banking online safely

Protect your identity and accounts while banking by computer

Financial education from *Consumer Action* and *Visa Inc.*

Paying a bill, depositing a check or conducting any other financial transaction used to require a trip to the bank or post office. Now technology makes it possible to bank and pay bills without leaving your home or office.

Online banking is safe and offers many advantages over branch banking. But that doesn't mean you should let your guard down. In addition to the many measures financial institutions take to keep out intruders, you have to take precautions to protect your personal data and accounts. Once you know what to watch for and what tools are available to enhance your security, you can enjoy the benefits of online banking without risk.

What is online banking?

Online banking, also known as Internet banking, lets you access your accounts and make certain transactions using a computer and Internet connection. Most financial institutions, including banks, credit unions, lenders and investment companies, offer online banking. There are even banks that only offer online accounts.

You can set up your current checking/savings accounts for online banking, or you can open a new account online. To open a new account, choose your institution. Bankrate.com allows you to compare checking and savings accounts available in your area. Once you choose a bank, you can go to its website and apply for an account. Typically, you will find online applications under "personal banking." You can open an individual or a joint account with another person. The application will ask you to:

- Provide your personal information, including name, address, phone number, Social Security number and ID, such as a driver's license number. For joint accounts, both applicants must provide this information.
- Fund your account with an initial deposit. Most banks require at least a "minimum deposit" to start but you can add as much money as you want. You can do this by providing the account number for an existing bank account or a credit card. You may be able to save your application and send a check in the mail if you can wait several days for the account to be opened.

The bank will send you documents to sign and return. You can mail them back.

Just because you apply for your account online does not mean you will have access to online banking. As with existing accounts, you may need to visit your financial institution's website and register for website access by providing your account details and email address, and choosing a username and password. During this process you may be asked to choose a photo and write a phrase to "authenticate" yourself and help you know you are at the right site when you log in. In addition, you may be asked to answer several secret questions in case you forget your username or password.

Generally, you can access checking and savings, credit card and mortgage accounts online.

Once your online account access is established, you can log into the system by entering your user identification (which might be your email address or username) and your password. If you have more than one account at one institution, such as a checking and a savings account, you can click on the account you want to access.

Depending on the institution and the types of accounts you have, while you are logged in you may be able to:

- check your current balance
- view account activity (deposits, withdrawals and payments)
- read and download your statements
- search for particular transactions (by date, amount, check number, or payee name)
- view canceled checks
- transfer money between accounts
- pay bills (you enter payee information and choose when the bills will be paid)
- view account terms (such as interest rates, fees and due dates)
- set and manage alerts, request a stop-payment, or order checks
- contact customer service by instant chat or secure email

> ***TIP:*** *Confused? Most financial institutions offer a "test drive" for online banking in the form of a video or virtual tour of the site. Watch and learn!*

To end your online banking session, sign off (or log out) and close your browser. If you walk away during a session, most financial services websites will log you out automatically after a period of inactivity. Log back in to continue.

Online banking benefits

Convenience is the main reason people bank online. With direct deposits and automatic bill payments, online banking customers can avoid going to a branch or mailbox. Most bank accounts come with an automated teller machine (ATM) card so you can get cash from an ATM or "cash back" on purchases (at the grocery store, for example). And, account information is available 24/7—no more waiting for the monthly statement.

> ***TIP:*** *Many financial institutions issue "debit cards," which can be used as an ATM card as well as to make purchases at stores and online. You can use your debit card with your PIN number or by signing your name.*

Lower cost is another benefit of online banking. Not only can you avoid the cost of postage to mail bills, you reduce the number of checks you have to buy. And "e-accounts"—accounts that require that all or most deposits and other transactions be made electronically—often are free or low-cost, even if you don't keep a minimum balance.

Online banking also is an environmentally friendly alternative to regular banking, since it requires less paper (fewer checks, and statements and bills can be delivered electronically) and no fuel.

Online banking risks

While there are many advantages to banking online, there may also be some disadvantages. These include:

- temporarily losing access to your account, either because you don't have access to a computer, the Internet connection is interrupted or the institution's website is "down"
- you miss a payment because you don't notice the email that alerts you to your online statements
- email "phishing" and other scams to convince victims to provide their log-in information
- failure to protect your usernames and passwords, which could allow a stranger to access your account

Safer online banking

Banks and other financial institutions work hard to ensure a safe, problem-free online banking experience. But there are things you can do to increase the likelihood that your personal information will remain private and your accounts will stay secure.

Make sure that any institution you do business with is legitimate. (A fancy website doesn't prove anything.) Start by reading about the bank in the site's "About Us" section, and then try to verify the information. For example, call the phone number provided. Also, do an online search to find any posts about the institution, including consumer complaints.

Bookmark your bank's site instead of typing in its Web address (URL) on each visit, as you could make a typo and end up on a "spoof" site designed to trick you into entering your login information. Before you set the bookmark, double-check to be sure you've typed the URL correctly.

Verify that the bank is insured. The FDIC name and logo indicate that the bank's customers will be reimbursed for losses on their deposits up to $250,000 if the bank fails. But don't just trust the presence of a logo on a website. Confirm that the institution is insured by visiting the FDIC's website (www.fdic.gov), where you can search by the bank's name, city, state or ZIP code. While a bank that is not FDIC-insured may be legitimate, its customers may not be covered in case of a loss. (Most brokerage accounts, such as your IRA account, are not FDIC-insured.)

computer, mobile device, accounts and apps and don't reveal them to anyone. Never save your password on sites with financial or personal information—including retailers who have your credit card on file. While it's a hassle, consider entering your payment card number each time you make a purchase instead of allowing the merchant to save it.

Log out. Never leave your computer or mobile device unattended while logged on to a banking or payment site or app. Sign out and close the app or browser window when finished with the session or when stepping away from the screen. If using a shared or public computer, clear your browsing history by clicking on the Tools menu in most browsers and selecting "Delete Browsing History" or "Clear Private Data."

Don't send sensitive data by email. Don't send personal information such as credit card numbers, passwords, your birth date or your Social Security number by email. Instead, log in to the company's website. Most companies that deal with sensitive information allow logged-in users to send secure mail to customer service and to receive an answer via the site.

Check website security. Verify that "https://" (not just "http://") is in the browser's address bar. All legitimate finance and retail websites use this SSL (Secure Sockets Layer) encryption to make it safe to bank or pay online.

Lock your wireless network. Leaving your wireless network "unlocked" means that anyone within range of your Wi-Fi signal can access it and possibly capture the data you send and receive on an unencrypted site. To secure your wireless network, password-protect your router.

Avoid shopping or banking in a public Wi-Fi hotspot. If you must use public Wi-Fi, make sure you are at a secure site (https://), disable file sharing, and use a VPN (virtual private network) such as Private WiFi (www.privatewifi.com) to protect your identity online.

Use a digital wallet. Your bank or payment processor may offer digital wallet service to allow you to make purchases online without having to enter credit card numbers or other payment information. The purchase is charged to your secure pre-registered account that is walled off from your network.

Do business only with individuals and companies you trust. Check the reputation (complaint history and customer satisfaction ratings) of any business that is new to you before you submit personal or payment information. You can get a lot of information through a simple online search for the company's name.

Vet your apps. Don't download an unfamiliar app until you've read user reviews and made sure the developer is legitimate. Read the developer's privacy policy for the app, which might be found under the "Settings" or "About This App" tab. TRUSTe certifies the privacy practices of mobile app developers as well as website owners, so look for the logo. If necessary, reset the app's privacy settings to a level you are comfortable with. Be aware that some apps need to track your location to be effective.

Be on guard for fraudulent communications. If you question the authenticity of an email message, text message or phone call, don't respond. Contact the company directly to verify. Legitimate businesses never contact you to ask for your Social Security number, username, password or other sensitive data. If you fall for a "phishing" email and recognize your mistake, immediately change the password on your account and notify the institution where you have the account. Take advantage of spam and phishing filters in your email service. Always type in the Web address of the site you want to visit rather than clicking on a link in an email, which could lead you to a bogus site.

Guard against malware. Use antivirus and antispyware and make sure they are updated regularly to avoid malicious software that can steal your information while you're online. Enable your computer's built-in firewall to create a virtual barrier between you and the Internet.

Delete old banking and transaction text messages. Old text messages that contain account balance or other private information should be deleted from your phone and synched devices.

Protect your device. Since smartphones and PDAs can store a great deal of sensitive information and are easily lost or stolen, it makes sense to put extra effort into protecting them. Use a password to lock the phone when not in use, and set the phone to lock after a certain number of minutes of being idle.

Erase your hard drive. Before selling, donating or disposing of your computer or mobile device, be sure to erase its hard drive. This entails more than just deleting files. Check the "Help" menu or the manufacturer's site for instructions, or contact your wireless carrier for help with a phone or PDA. ReCellular (www.recellular.com/recycling/data_eraser/default.asp) provides instructions for erasing many phone models. If your employer provided the phone or computer, contact the person on staff who is in charge of technical issues. Be aware that your employer has the right to access information stored on company-owned devices.

Assistance and information

Federal Trade Commission www.ftc.gov

The FTC educates the public about how to protect themselves in the marketplace and takes complaints about businesses that violate consumers' rights and privacy.

Consumer Action

www.consumer-action.org
Consumer advice and referral hotline:
hotline@consumer-action.org or 415-777-9635
Chinese, English and Spanish spoken

Consumer Action created the Digital Dollar series with funding from Visa Inc.

VISA

consumer action
Education and advocacy since 1971

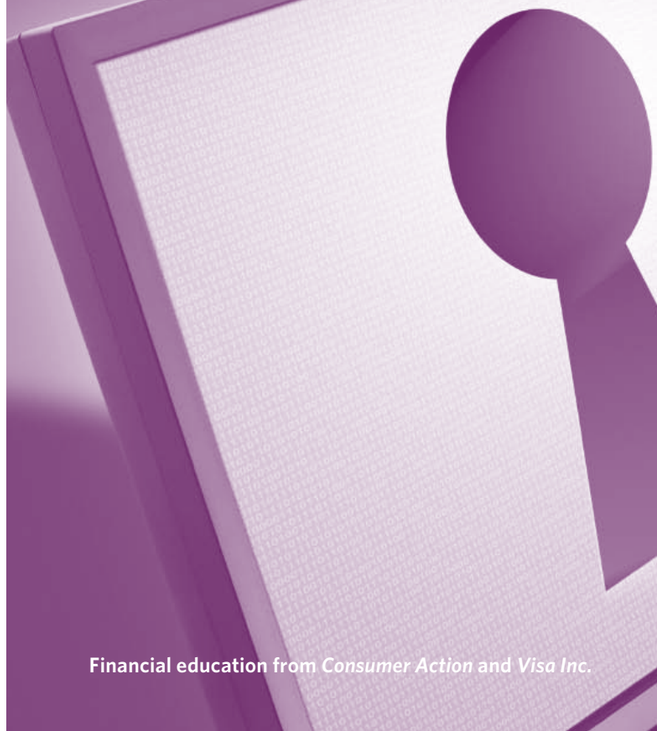
Visit Visa's financial education program, Practical Money Skills, at: ***www.practicalmoneyskills.com***

Find tips and practical know-how for protecting account information, avoiding payment card scams, and resolving unauthorized card use in English and Spanish at: ***www.visasecuritysense.com***

Your Digital Dollars

Safety and privacy in online and mobile transactions

Protect your identity and data while banking or paying digitally



Financial education from *Consumer Action* and *Visa Inc.*

As more daily tasks, from shopping and banking to working and socializing, get done on a computer or mobile device, the opportunities to expose personal data increase.

While many security measures enhance the safety of digital transactions, online and mobile consumers may still face privacy risks. An open Wi-Fi connection, a lost smartphone or an accidentally revealed password are just a few of the ways your information could get out without your permission. Fortunately, there are many tips and tools to help you make safe and secure transactions online and on the go.

Why is online and mobile security important?

While the Internet and mobile technology have improved our lives in many ways, they also have created new ways for consumers' personal information to be stolen, unintentionally revealed, or misused. For example, an identity thief anywhere in the world could steal your personal information by luring you to a fraudulent website that tricks you into revealing your password. A lost or stolen smartphone full of stored passwords and account information could pose more risk than a missing wallet. And if your information is sold to third parties by a website you've visited, you could receive frequent (and perhaps annoying) marketing emails (spam), or even unauthorized charges.

The good news is, you can avoid these and other potential problems by being cautious and staying informed.

Risks for online and mobile consumers

Everyone runs the risk of having a piece of mail intercepted or a confidential conversation overheard. But if you bank or make payments online or by mobile device, there are other ways your privacy could be violated.

Someone who ends up with your lost or stolen computer or phone might be able to access your personal data, account numbers and payment information.

Someone could intercept the Information you send and receive over a wireless network.

A scammer could trick you into entering your private information on a spoofed (copycat) website or responding to a bogus email request (phishing).

A data breach (the theft or unintentional release of information held in an institution's database) could result in your and other customers' information landing in the hands of a thief.

Someone you know could access your accounts by guessing or discovering your password. Or you may save usernames and passwords on a shared computer or unprotected mobile device, giving a key to intruders.

Your computer or mobile device could be infected by spyware or other disruptive software (malware) capable of stealing your data.

Your information, gathered by a business, could be sold or given to one or more third parties for marketing or other purposes. There even have been cases of sharing payment card information between businesses, resulting in unauthorized charges.

What to look for in providers and products

One of the best ways to protect your personal data is to deal only with financial institutions, merchants, app developers and others who work hard to protect the security and privacy of their customers and website visitors. When considering a company, product or service, look for:

Legitimacy: A fancy website doesn't make a business legitimate or trustworthy. If you're not familiar with a company's reputation, check its authenticity, customer satisfaction rating and complaint history through an online search. Verify information and claims (for example, call the phone number listed).

Encryption: A closed padlock or unbroken key in the browser frame and an "s" after "http" ("https://") in the website address indicate the site is secure and encrypted. (This means the information is being sent in a format that only the intended recipient can read). Logos from companies such as VeriSign and McAfee signify that a website uses encryption or other security technology to protect your data. Click on the logos for more information about the site.

Extra security features: A site that automatically ends your banking session after a certain period of inactivity is an example of an extra measure of security. This prevents someone from accessing your account if you walk away from the computer without logging out or closing the browser window. Another good sign is a log-in that requires "double" authentication, such as a photo you choose and a description you write about it, as well as a user-name and password.

A 'zero liability' policy: This guarantees you won't owe anything as a result of unauthorized activity, and that any money taken from your account will be replaced.

A strong privacy policy: A privacy policy, which explains how customers' personal information is collected, used and stored, should be clearly posted on the company's website. Ideally, it should state that the company won't share your information with third parties (unaffiliated individuals or organizations). If necessary, you should be able to easily "opt out" of having your information shared. Logos from organizations such as TRUSTe or BBBOnline signify a trustworthy or reasonably strong privacy policy. (Click on the seal to verify it's legitimate—the address that appears should match the address of the official certifying company website.) Leave the site if you are not satisfied that your privacy will be protected.

The collection of consumer information is not necessarily a bad thing. Many reputable companies and merchants use the information they gather to improve customer service and efficiency, making your online or mobile experience more pleasant and productive. However, some companies use consumer information for aggressive marketing efforts, sell the data to one or more third parties, or fail to protect the data from hackers, dishonest employees or others who would misuse it. Caution is the best policy when deciding who to give your business to and how much personal information to reveal.

Tips for protecting your privacy

Reveal only what is necessary. When registering for an online service or account, fill out only those fields in the registration form that are required to use the service or open an account. (These are usually marked with an asterisk.) If given a choice, select options that result in less of your personal information being shared. Entering online contests and filling out forms for free trials or coupons may result in your information being sold or shared for marketing and promotions.

Take advantage of browser capabilities. Newer Internet browsers have built-in features that, when enabled, can help protect your privacy. For example, some browsers warn you when you are about to navigate to a site that may be fraudulent. Read the Help section of your browser for more information, and update your browser software regularly to take full advantage of new privacy features as they become available.

Manage your cookies. Cookies are small files stored on your computer by websites you visit. They track your activity while at the site. This information often is used to target marketing efforts, but it also is used for things like remembering items in your shopping cart and recognizing you as a repeat visitor. You can set your browser to delete cookies automatically whenever you exit, or to not accept cookies at all. Instead, consider enabling or disabling cookies on a site-by-site basis. Check the Help section of your browser for instructions.

Protect your passwords. Create strong passwords for your

Your Digital Dollars

Online and mobile banking and mobile payments

Lesson Plan and Class Activities

A Consumer Action Training Guide

Your Digital Dollars:
Online and mobile banking and mobile payments

Lesson Plan and Class Activities

A Consumer Action Training Guide

Lesson Purpose:

To make participants aware of how online and mobile banking and mobile payments work, to help them understand what the advantages and disadvantages of banking or paying electronically might be, and to provide them with the knowledge and tools that will enable them to protect their assets and their privacy while banking and paying online and on the go.

Lesson Objectives:

By the end of the lesson, participants will understand:

- what online banking, mobile banking and mobile payments are.
- what sorts of transactions are possible, who offers online and mobile banking and payment services, and what tools and information are needed to be able to bank or pay digitally.
- what the various online and wireless banking and payment platforms are and what capabilities are available with each.
- the benefits and risks associated with banking and paying digitally.
- how to protect their personal information, device data and accounts.
- what to look for in financial institutions, online merchants and mobile app providers.
- how to enhance the security of every online or mobile transaction.
- what resources are available to provide additional information and assistance.

Lesson Duration:

2½ hours (plus a 10-minute break)

Materials:

For instructor:

- Brochures:
  - *Banking online safely: Protect your identity and accounts while banking by computer*
  - *Mobile banking and mobile payments: Making financial transactions safely on the go*
  - *Safety and privacy in online and mobile transactions: Protect your identity and data while banking or paying digitally*
- Lesson plan (pages 3-16)
- Activities (including answer keys) (pages 17-22)
  - What's "Phish-y" About This? (pages 17-20)
  - Mobile Banking and Payment Safety (pages 21-22)
- Evaluation form (page 23)
- Visual teaching aid (PowerPoint presentation with instructor's notes)

Instructor will also need:

- a computer and projector for the PowerPoint presentation (optional). (The PowerPoint slides also can be printed on transparent sheets for use on an overhead projector.)
- an easel and pad, or a whiteboard, and markers.

For participants:

- Brochures:
  - ***Banking Online Safely:*** *Protect your identity and accounts while banking by computer*
  - ***Mobile Banking and Mobile Payments:*** *Making financial transactions safely on the go*
  - ***Safety and Privacy in Online and Mobile Transactions:*** *Protect your identity and data while banking or paying digitally*
- Activities:
  - What's "Phish-y" About This? (2 pages)
  - Mobile Banking and Payment Safety (1 page)
- Evaluation form (1 page)
- OPTIONAL: Printout of the PowerPoint presentation

Lesson Outline

- Welcome (5 minutes)
- Online Banking (10 min)
- Mobile Banking (10 min)
- Mobile Payments (15 min)
- What to Know About Digital Banking and Payments (10 min)
- Activity: What's "Phish-y" About This? (15 min)
- Break (10 min)
- Protecting Your Mobile Device and Data (10 min)
- Online Banking Precautions (10 min)
- Vetting Financial Institutions, Online Merchants and App Providers (5 min)
- Avoiding Scams, Fraud & Malware (10 min)
- Guarding Your Data (10 min)
- Activity: Mobile Banking and Payment Safety (15 min)
- Assistance & Resources (10 min)
- Questions & Answers (10 min)
- Wrap-up and Evaluation (5 min)

Financial education from Consumer Action and Visa Inc.

Instructor's Notes:

This "Your Digital Dollars" training module, consisting of three brochures (*Banking Online Safely: Protect your identity and accounts while banking by computer; Mobile Banking and Mobile Payments: Making financial transactions safely on the go; and Safety and Privacy in Online and Mobile Transactions*: *Protect your identity and data while banking or paying digitally*), a lesson plan that includes class activities, and a PowerPoint presentation, was created by the national non-profit organization Consumer Action in partnership with Visa to be used nationwide by non-profit organizations providing personal finance, consumer and housing education in their communities.

Before conducting the training, familiarize yourself with the three brochures, the lesson plan (including activities), and the PowerPoint visual teaching aid.

The PowerPoint presentation contains notes for each slide (appearing below the slide when in Normal view or Notes Page view, and inserted into the lesson plan). These notes offer detailed information about the items appearing on the slide. The lesson plan includes indicators so you will know which slide corresponds to each part of the lesson, and when to move to the next one.

Why Adults Learn, a PowerPoint training for educators, provides tips for teaching adults and diverse audiences—it will be helpful to you even if you have taught similar courses before. The slide deck is available at the Consumer Action website (http://www.consumer-action.org/outreach/articles/why_adults_learn/).

Welcome (5 minutes)

➡**SLIDE #1** (onscreen as participants arrive; direct participants who arrive early to beginning reading the three brochures)

Welcome participants. Introduce yourself and present the purpose of the training and the agenda.

Review the contents of participants' packets. Ask the class to take a look inside their packets and make sure they have all the materials needed.

If you have a small group, you can ask individuals to introduce themselves and tell you what they hope to get out of the training. In a larger group, invite volunteers to share their expectations. On your whiteboard or easel pad, jot down some of the specific things participants mention. You can come back to this at the end of the training to make sure you've covered these points. (This activity is designed to serve as a brief icebreaker. It will also give you an idea what participants' expectations and needs are.)

Ask: When is the last time you saw a line *inside* a bank branch (not at the ATM!), or the last time you wrote a check for an everyday purchase? Fewer customers visiting the bank and fewer checks changing hands are just two signs that more consumers are using technology to manage their finances and make purchases. Today we'll be learning about:

- how you can do your banking online or on your mobile device;
- the different types of financial transactions that are possible with a mobile device;
- the advantages and disadvantages of banking and paying electronically; and,

- how to protect your assets and your privacy while banking and paying online and on the go.

Online Banking (10 minutes)

Introduction: Online banking is sometimes referred to Internet banking or e-banking. It makes it possible for you to access your financial accounts and conduct certain transactions using your computer and a high-speed, or broadband, Internet connection.

Ask: *What kinds of banking tasks can you do online?* (Allow time for responses. You can jot them down on your easel or whiteboard, if you like.)

➡SLIDE #2

Go over slide bullet points, referring to slide notes for further explanation/examples for some of the items:

- Being able to search for transactions by date, amount, check number or other criteria is useful if you need proof that you made a payment or deposit.
- Being able to view canceled checks is useful if you forgot to enter the check in your check register and can't remember whom it was made out to.
- To use online bill-pay services, you enter payee information (name, address and account number) and the amount of the payment. The payee stays in your list to be used monthly or as needed. You can set up automatic recurring payments, too.
- Account terms include such things as interest rate and payment due dates for loans (when you are on, say, your mortgage lender's site or the site of the lender who has your auto loan).
- Alerts are text or email messages that notify you of certain account activity or status. For example, you might choose to get an alert when your account balance drops below a certain amount, when a direct deposit is made to your account, or when a check clears.

Ask: *What kinds of alerts would you find helpful in managing your money, your bank accounts and your bills?* (Different financial institutions offer different types of alerts, and many credit card issuers, phone service carriers, lenders, and others also offer alerts that notify you, for example, when your new statement is ready, when the bill is due, when you are approaching your limit, and more.)

➡SLIDE #3

Go over slide bullet points.

After reading the last bullet point, ask: *Would you feel comfortable putting your money in a bank that offered only online access, and did not have branches you could visit?* (Allow a moment for class input.)

Explain that there are a number of reputable banks that operate only online. Since these banks have lower overhead costs (no branches to open, maintain and staff), they often pass those savings on to customers in the form of no or lower fees and/or interest paid on the account. If you're interested in an Internet-only account, look for one that waives or reimburses some or all the fees you'll be charged for using other banks' ATMs. And, if you plan to make check deposits

(instead of direct deposit), make sure the bank offers an app that allows you to do so by taking a photo of the check with your smartphone. This is not a good option for customers who have to deposit cash.

➡SLIDE #4

The online banking process is pretty similar regardless of which financial institution you have your account at.

Go over slide bullet points, referring to slide note:

- You must register before you can begin banking online. That entails setting up your login information, which typically is either a username you create or your email address, and a password you create. If you have more than one account with the institution, you will be given the option to select the one you want to work with now.

Ask: *What are the advantages of being able to do your banking online?* (Allow time for responses. Jot down answers on your whiteboard or easel.)

➡SLIDE #5

Go over slide bullet points, referring to slide notes:

- Banking anytime, anywhere, as long as you have Internet access and a computer.
- Direct deposit is safer, faster and more convenient than handling a physical check. Cash can be gotten from an automated teller machine (ATM) or as part of a debit card purchase (at the grocery store, for example, by requesting “cash back”).
- Savings include the cost of stamps to mail bills, the cost of checks, and the cost (in time and gas) of trips to the bank, post office or mailbox.
- Checking your account frequently online is not only convenient, it’s a good way to spot any errors or signs of fraud sooner rather than later. And it can help you avoid overdrawing your account.
- Many e-accounts—accounts that require transactions be conducted online or at the ATM—are fee-free or charge only a small monthly fee.
- Online banking is green: no paper account statements, and you may also be able to sign up to receive e-bills; fewer or no checks and envelopes; and, no gas used for trips to the bank, post office or mailbox.

Mobile Banking (10 minutes)

Introduction: Mobile banking is sometimes referred to as m-banking. It makes it possible for you to access your financial accounts and conduct transactions wirelessly, using your mobile device. It’s no longer impossible to deposit a check while sitting on a beach or to pay the electric bill while sightseeing halfway around the world.

Ask: *What kinds of banking tasks can you do using a mobile device?* (Allow time for a few responses.)

➡SLIDE #6

Go over slide bullet points, referring to slide note:

- Exactly what you are able to do from a mobile device depends on the type of phone, smart device, tablet computer or PDA (personal digital assistant) you have; your wireless service plan; and the technology used by the financial institution. A smartphone with data service is required to take advantage of the most advanced mobile banking capabilities.

➡SLIDE #7

Go over slide bullet points, referring to slide notes:

- Banking by text message is limited to getting information about your account (such as your balance) and receiving text alerts.
- Online banking via mobile device is similar to online banking via computer: You use the device's Web browser to log in to your account, and then you can conduct all the same transactions as you can on your computer.
- An app typically is faster to use and easier to navigate on a small screen than a website.

Mobile Payments (15 minutes)

Introduction: Mobile payments, or m-payments, are payments you make using your mobile device instead of writing a check, handing over cash, or pulling out a credit or debit card.

Ask: *Have any of you ever made a payment or purchase with your mobile phone or PDA? Where was it? What did you like about it?* (Allow time for a few responses.)

➡SLIDE #8

Go over slide bullet points, referring to slide notes:

- When shopping using an app or the Web browser on your mobile device, the purchase amount typically is charged to a credit or debit card, a pre-registered Internet payment service account (such as PayPal) or a "digital wallet" (a service that stores your payment and shipping information for electronic transactions).
- Sometimes called "text to buy," a text (SMS) transaction might be added to your wireless service bill or charged to a pre-registered credit or debit card, Internet payment service account or digital wallet. This type of mobile payment typically is used for small amounts, such as the cost of downloads (ringtones and songs, for example), parking fees, transportation fares and movie tickets, though it is even possible to authorize a payment to family members in another country by text message or to buy big-ticket items from certain retailers.
- Direct mobile billing (less common) allows you to have purchases added directly to your wireless service bill at checkout if the option is available.
- P2P payments are typically small, informal transactions between two people—for example, paying the gardener or covering your share of a dinner bill. The payment may be made using an app or, less common at this point, by touching two smartphones together.

- Proximity (indicating “close”) payments make it possible to make purchases at the cash register or other point of sale (POS) simply by tapping or waving your mobile device close to an electronic reader. This payment option is becoming more widely available as more phone manufacturers and merchants install the necessary chips and chip readers.

Review of banking and payment types:

➡SLIDE #9

Read each statement and have participants identify which type(s) of banking or payment type the statement describes—there may be more than one correct answer to each item. You can call on volunteers or invite the class to call out responses.

1. I can check my balance 24/7. (online banking and all types of mobile banking—text/SMS, mobile Web browser and mobile app)

2. My banking capabilities are limited. (text (SMS) banking)

3. I can pay my bills anytime. (online banking, mobile Web and mobile app)

4. My banking activity could cost me money. (any type of mobile banking if you exceed the text or data service included in your regular monthly wireless service plan)

5. I bought a new sweater using my mobile phone. (mobile Web payment)

6. I paid for my coffee by waving my mobile phone near a machine. (mobile point-of-sale (POS/proximity) payment)

7. I paid my babysitter. (mobile peer-to-peer (P2P) payment)

8. I entered a code and purchased a new ringtone. (mobile text (SMS) payment, or “text to buy”)

9. I bought something and the charge was added to my wireless bill. (direct mobile billing or, possibly, mobile text (SMS) payment)

10. I can deposit a check by taking a picture of it. (mobile app banking)

11. I have to sign out or log off to end this type of banking session. (online, mobile Web and mobile app)

12. I have to visit the financial institution’s website. (online banking and mobile Web banking)

13. What I can do depends on the type of device I have. (mobile banking and mobile payments—text banking and text payments are the only two that are possible with virtually any device)

14. I have to complete the enrollment and setup process on a computer. (online banking and mobile Web or mobile app banking)

15. I need to download a special program first. (mobile app banking)

16. This type of banking can be done using virtually any mobile phone. (text (SMS) banking)

17. This type of banking requires an Internet connection. (online, mobile Web and mobile app)

18. I may be able to send money to my family back home by entering a code. (mobile text (SMS) payment)

19. I can make these types of payments using a digital wallet. (mobile Web, mobile text (SMS) and mobile peer-to-peer)

What to Know About Digital Banking and Payments (10 minutes)

Introduction: Making mobile purchases and payments or banking online or by mobile device isn't particularly risky, but that doesn't mean that it's absolutely risk-free, either. It's important for anyone who uses online or mobile banking and payment technology to be aware of the potential drawbacks.

Ask: *What do you think some of the potential risks or issues could be when banking and paying online or wirelessly using a mobile device?* (Allow time for a few responses. Write responses on whiteboard or easel, if you like.)

➡SLIDE #10

Go over slide bullet points, referring to slide notes:

- It's possible to temporarily lose access to your accounts if you're outside a wireless coverage area, your phone battery is dead, you don't have access to a computer, the Internet connection is interrupted or the institution's system is "down."
- Bill payments could arrive late because there is not enough time between when you request the payment and when the bank makes the electronic transfer or mails the check.
- It's far more likely that you would lose your mobile device than, say, a desktop computer. A lost phone would not only be inconvenient, it could leave your personal data, account information and purchase ability accessible to someone who finds it.
- Anytime you send sensitive information over an unsecured wireless network there's the possibility that it could be exposed.
- Your personal data or your accounts could be accessed without your permission as the result of a data breach (the theft or unintentional release of information held in an institution's database) or because someone has obtained your username and password.
- Your computer could become infected with malware (viruses, spyware and other code designed to steal your information or do harm to your device or data). Though not a major issue for mobile devices so far, malware could hit phones more widely in the future. Antivirus and firewall protection is not yet widely available for mobile devices. Or you could become the victim of a phishing attempt (trying to get you to reveal your password or other sensitive data) or other scam (such as a "spoofed" website).
- It's possible that your information could be collected and used for marketing purposes or sold to a third party. This could result in nuisance email messages, pop-up windows and other annoying marketing efforts.

- If you pay for wireless service per unit (text message or megabyte of data), or if you use more text messages or data than is included in your monthly service plan, or if you use your service while roaming outside your carriers' network, the activity on your mobile device could increase your monthly service bill.

Activity: What's 'Phish-y' About This? (15 minutes)

➡SLIDE #11

Have participants remove the *What's "Phish-y" About This?* activity from their packets.

This activity can be done individually or in small groups. Instruct participants to circle any "red flags"—things that tip them off that the message is phishing for personal information or the website could be "spoofed."

Allow 5 to 10 minutes to complete the activity.

If the activity was completed individually, invite participants to raise their hands if they would like to answer. If the activity was done in groups, rotate among them, giving a spokesperson from each group the opportunity to answer when it is that team's turn.

Refer to the answer key provided for the list of red flags and additional information.

Break (10 minutes)

Announce a 10-minute break. Make yourself available for a few minutes to direct people to the restroom or a place to get drinks and snacks.

Leave the following slide onscreen during the break.

➡SLIDE #12

Protecting Your Mobile Device and Data (10 minutes)

Introduction: The more you do online or on your mobile device, the more opportunity there will be for your personal data to be unintentionally exposed, stolen or misused. You can greatly reduce the odds of that happening by being careful, and by taking steps and using tools to enhance security.

➡SLIDE #13

Depending on how you use your mobile device, it might be less like a phone and more like a wallet that can make calls. Since your mobile device may contain information that someone could use to make purchases or access your accounts, it makes sense to put extra effort into keeping it safe and secure.

Go over slide bullet points, referring to slide notes:

- Don't leave your mobile device unattended or accessible to anyone else. Don't lend your phone to anyone you don't know and trust.
- Old text messages that contain online banking or purchase/payment transaction messages that you would not want someone else to see could still reside on your

device. (This information may also be saved on your computer if you "sync" your phone with your computer.) Delete sensitive messages regularly.

- Don't save your account numbers or access information anywhere on your mobile device where someone could get to it.
- Use a password to lock the phone when it's not being used, and set the phone to automatically lock after a certain number of minutes of being idle.
- There are many software products available that help owners locate (track) their missing device or "wipe" their data remotely if the device is ever lost or stolen.
- If you lose your phone, contact your wireless service carrier immediately to suspend your service. Then use a computer to log on to your financial accounts and deactivate text banking, change passwords and otherwise secure your accounts. (You also may be able to do this by calling your bank.)
- This entails more than just deleting files. Check the "help" menu or the manufacturer's site for instructions, or contact your wireless carrier for help with a phone or PDA.

Online Banking Precautions (10 minutes)

Introduction: Financial institutions put a great deal of effort into making online banking and other online transactions as secure as possible. But there's a lot you can do *yourself* to increase the likelihood that your personal information will remain private and your accounts will stay off limits to others.

Ask: *What sorts of things could you do to make your online banking experience problem-free?* (Allow time for responses, before revealing the next slide.)

➡SLIDE #14

Go over slide bullet points, referring to slide notes:

- If there's any doubt in your mind about the legitimacy of the financial institution, take the time to check it out before you put your money there. Read about the bank in the site's "About Us" section, and then try to verify the information. For example, call the phone number provided. Also, do an online search to find any posts about the institution, including consumer complaints. Don't be fooled by a fancy website.
- Confirm that the institution is insured by the Federal Deposit Insurance Corporation (up to $250,000) by visiting the FDIC's website (www.fdic.gov), where you can search by the bank's name, city, state or ZIP code. While a bank that is not FDIC-insured may be legitimate, its customers may not be covered in case of a loss. The NCUA administers the National Credit Union Share Insurance Fund (NCUSIF), which provides deposit insurance for credit unions much like the FDIC does for banks. Visit the NCUA site (www.ncua.gov), or call, to find out if the credit union you're considering joining is insured.
- Don't spend money before it's available or your checks/payments may bounce and you may be charged an overdraft fee.
- Know how much time it takes your bank to get a payment to your creditors after receiving your online bill payment request. Some payments, typically to larger creditors, are made electronically and may reach their destination within a couple of days of your request. Payments to smaller creditors, such as your dentist, may take as long as a

week or more because the bank must write a check and mail it to the recipient. Leave plenty of time for payments to reach creditors by the due date.

- For example, what does their privacy policy say about how they'll use your personal information? Do they offer a zero-liability guarantee for any unauthorized transactions? Will they reimburse any late fees if they don't make your requested bill payment as scheduled?
- You'll detect fraud sooner rather than later. And, in most cases, you must report unauthorized account activity within a certain time period (say, within 60 days of when the transaction posted) to be protected by a zero-liability guarantee.
- Mobile banking activity may cost you money in higher wireless service bills. If so, consider banking online from your home computer, or inquire about other wireless service plans that better accommodate your usage.
- If you must use public Wi-Fi, take precautions. Look for the closed padlock or unbroken key in the browser frame and an "s" after "http" (in other words, "https://") in the Web address, which indicates an SSL (Secure Sockets Layer) connection. Use VPN software or a hosted VPN service to set up a "virtual private network," which provides encryption over an unencrypted Wi-Fi connection.

Vetting Financial Institutions, Online Merchants and App Providers (5 minutes)

Introduction: Using a mobile device means you may be doing everything from banking and shopping online to making instant payments or buying apps, ringtones and other products. It can become second nature to simply click a button and make a purchase or payment. But it's important to know just who you're giving your money—and your personal and account information—to and that they are trustworthy.

Ask: *What do you need to know to feel comfortable giving your business to a financial institution, merchant or software developer?* (Allow time for responses before revealing the answer on the next slide. Jot down learners' responses on your whiteboard or easel pad, if you like.)

➡SLIDE #15

Go over slide bullet points, referring to slide notes:

- A fancy website doesn't make a business legitimate or trustworthy. If you're not familiar with a company's reputation, check its authenticity, customer satisfaction rating and complaint history through an online search before you submit personal or payment information. Verify information and claims (for example, call the phone number listed).
- Make sure you will receive a receipt, and then keep it until you receive, and are satisfied with, your purchase.
- What happens if you no longer want your purchase after you receive it? Will you be allowed to get a refund? Store credit? Or are all sales final? Who pays for return shipping, if you have to mail the item back? How long will it take to process your return and issue the refund or credit? Make sure you are satisfied with the return process *before* making your purchase.
- This guarantees you won't owe anything as a result of unauthorized transactions on your account and that any money taken from your account will be replaced. Your wireless carrier and other payment processors all have policies for disputing unauthorized

charges, but not all companies offer zero liability. When you have the option, use a credit or debit card with a "zero liability" policy. Generally speaking, credit cards offer the greatest consumer protections in case your purchase is unsatisfactory or undelivered, or if you have a billing dispute with the merchant.

- A closed padlock or unbroken key in the browser frame and an "s" after "http" ("https://") in the website address indicate the site is secure and encrypted (in other words, the information being sent is encoded so that only the intended recipient can read it). Logos from companies such as VeriSign and McAfee signify that a website uses encryption or other security technology to protect your data.
- A site that automatically ends your shopping or banking session after a certain period of inactivity is an example of an extra measure of security. This prevents someone from accessing your account if you walk away from the computer without logging out or closing the browser window.
- A privacy policy, which explains how customers' personal information is collected, used and stored, should be clearly posted on the company's website. Ideally, it should state that the company won't share your information with third parties (unaffiliated individuals or organizations). At the very least, you should be able to 'opt out" of having your information shared. Logos from organizations such as TRUSTe or BBBOnline signify a trustworthy or reasonably strong privacy policy. (Click on the seal to verify it's legitimate—the address that appears should match the address of the official certifying company website.) Leave the site if you are not satisfied that your privacy will be protected. If you're downloading an app, you may be able to reset the app's privacy settings to a level you're comfortable with. Be aware that some apps can track your location. Also be aware that information gathering done directly by a third party operating on the site (such as the sponsor of a pop-up ad), or one whose site you land on by clicking a link, is subject to that company's own, possibly weaker, privacy policy.

Avoiding Scams, Fraud and Malware (10 minutes)

Introduction: Technology can be very freeing—you can do more, faster, from just about anywhere, at any time of day or night. But not everyone you might come into contact with while using you computer or wireless device is trustworthy.

➡SLIDE #16

Go over slide bullet points, referring to slide notes:

- Phishing attempts try to get you to reveal sensitive information by making you believe you are communicating with a legitimate business, such as your bank. Keep the contact number, email and short code (text) for your bank and other institutions you do business with in your address book so you'll see the name come up when you get a legitimate call, email or text message.
- Phishing emails often include a link to a spoofed, or fraudulent, website. A spoofed website is a copy of a legitimate site designed to lure you into revealing your password and other sensitive information. Rather than clicking a link in an email or text message, bookmark the company's website while on the legitimate site and use that to get there. That way you'll also avoid the possibility of mistyping the web address, or URL, and landing on a spoofed site that takes advantage of customers who misspell the institution's URL.

- If the source of an app is unknown, do an online search for reviews and user feedback to find out if others have had problems with the app or the merchant.
- If you question the authenticity of an email message, text message or phone call, don't respond. Contact the company that the message is supposedly from directly to verify the legitimacy of the communication. Remember, a legitimate business will not ask you for your Social Security number, username, password or other sensitive data via a communication you didn't initiate. If you've already responded to a "phishing" email (one that fishes for your information), immediately change the password on your account and notify the institution where you have the account.
- All major email service providers offer tools for filtering out spam and phishing messages.
- Newer Internet browsers have built-in features that, when enabled, can help protect your privacy. For example, some browsers warn you when you are about to navigate to a site that may be fraudulent. Read the user manual for your browser for more information. And update your browser software regularly to take full advantage of new privacy features as they become available.
- Use anti-spyware and antivirus software and make sure they are updated regularly to avoid malicious software that can steal your information while you're online. Enable any built-in firewall—a virtual barrier between you and the Internet—your computer or device might have.

Guarding Your Data (10 minutes)

Introduction: Your personal data—the private information that could be used to access your various accounts (not just financial, but phone, medical, and even credit reports, etc.)—are very valuable. Since a Social Security number, your mother's maiden name, or a password may be all that stands between a thief and your accounts, it's worthwhile to put some extra effort into guarding that information.

➡SLIDE #17

Go over slide bullet points, referring to slide notes:

- Passwords should be at least eight characters long and use a combination of uppercase and lowercase letters, numbers and symbols. Don't make a password out of a pet's name, birthdate, or other personal information. Strong passwords should be used for your device (to turn it on or wake it up from sleep mode) and for all your banking/financial and payment apps.
- Don't share logon info, including passwords, personal identification numbers (PINs), usernames or the answers to "password hints" with anyone—resulting transactions will be considered authorized by you—and don't leave them where someone could find them. Don't use the "remember me" function or similar options to store passwords or payment information on sites or in apps. Change your password regularly and change it immediately if you think it's been compromised.
- Log off financial and payment sites when you are done with your session or if you have to step away from the computer, and close the browser window after signing off. Clear your "cached" activity on a shared computer by clicking on the "Tools" menu (in most browsers) and selecting "Clear Recent History" or something similar. (The words may be slightly different depending on the browser you use.)

- Bluetooth is short-range wireless network technology. Headsets that don't have to be plugged into the mobile device typically use Bluetooth technology. Turn off Bluetooth whenever you are not using the device, and lock it so that it can't be opened without the password.
- Email and instant messaging aren't automatically encrypted, so don't send personal information such as credit card numbers, passwords, your birthdate or your Social Security number unless you are using a service or tool that offers the ability to encrypt the message.
- Lock your home wireless network so that strangers within range or your signal can't access your Wi-Fi (wireless Internet) connection and possibly capture the data you send and receive on an unencrypted site. Do this by creating a strong password for your router and enabling its built-in encryption tool.
- If you must use public, non-password-protected Wi-Fi, make sure you are at a secure site (https://), disable file sharing, and use a VPN (virtual private network) such as "Private WiFi" to protect your identity online.
- Also known as an Internet payment service, a digital wallet enables you to make purchases online without having to enter credit card numbers or other payment information. The purchase is charged to your pre-registered account.
- Use a firewall, which is a virtual barrier between your computer and the Internet. Your computer's operating system (OS) may have a built-in firewall; make sure it's turned on.
- Don't open anything that is not from a trusted source. Don't open files or click on links in chain letters or other unsolicited or questionable email.
- When registering for an online service or account, fill out only those fields in the registration form that are required to use the service or open an account. (These are usually marked with an asterisk (*).) If you're given the opportunity to change your privacy settings, select options that result in less of your personal information being shared, at least in the beginning. Entering online contests and filling out other optional forms increases the chances that your information will be used for marketing or other purposes, sometimes by third parties that buy the information.
- Cookies are small files stored on your computer by websites you visit. They track your activity while at the site. This information often is used to target marketing efforts, but it also is used for things like remembering items in your shopping cart and recognizing you as a repeat visitor. You can set your browser to delete cookies automatically whenever you exit, or to not accept cookies at all, but these options may restrict you from visiting certain sites or may diminish site functionality. Consider enabling or disabling cookies on a site-by-site basis. Check your browser user manual for instructions.

Activity: Mobile Banking and Payment Safety (15 minutes)

➡SLIDE #18

Have participants remove the *Mobile Banking and Payment Safety* activity from their packets.

This activity can be done individually or in small groups. Instruct participants to write the correct word or phrase to clarify each statement.

Allow 5 to 10 minutes to complete the activity.

If the activity was completed individually, invite participants to raise their hands if they would like to answer. If the activity was done in groups, rotate among them, giving a spokesperson from each group the opportunity to answer when it is that team's turn.

Refer to the answer key provided for the correct word or phrase to complete each statement.

Assistance & Resources (10 minutes)

Introduction: There are a number of resources that could be helpful to you as you start banking online or banking and making payments by mobile device.

➡SLIDE #19

The resources on this list can help you with specific issues regarding getting started, resolving a transaction dispute, or dealing with a service issue.

Go over slide bullet points, referring to slide notes:

- Whether you're already an online or mobile banking customer or just getting started, you can contact your financial institution's customer service or tech support departments directly for guidance.
- Contact the app vendor or developer or the company with which you use the app regarding any mobile payment questions or issues.
- If you're dissatisfied with a purchase, try first to resolve the issue directly with the merchant.
- If you aren't able to come to an agreement with the merchant and you want to dispute a transaction, contact the credit card company or financial institution that issued the card you used to make the purchase.
- If your payment was processed through an intermediary, such as an Internet payment service account or your wireless service provider, follow that company's instructions for filing a dispute.

➡SLIDE #20

If you'd like more information about Internet safety, protecting your privacy and personal information, avoiding scams, and choosing a reputable merchant or financial institution, the resources on this list can help.

- OnGuard Online: The U.S. federal government and the technology industry provide information and tips to promote online safety and security.
- PRC: The nonprofit Privacy Rights Clearinghouse offers a library of information, from tips for protecting your privacy online to how to shop safely on the Internet.
- FTC: The FTC educates the public about how to protect themselves in the marketplace and takes complaints about businesses that violate consumers' rights and privacy.
- FDIC: Read the Federal Deposit Insurance Corporation's tips for safe Internet banking and find out if the bank you're considering doing business with is insured.
- NCUA: Find out if a particular credit union is insured and get fraud prevention and personal money management tips from the National Credit Union Administration.

- MS: Learn how to create strong passwords, and use a tool to check the strength of your passwords.
- Visa: Financial education at the Practical Money Skills website and advice and tips for safety and security online at the company's Security Sense website.

Questions & Answers (10 minutes)

Preparation: Review the three *Digital Dollars* brochures.

Open the floor to questions.

Wrap-up and Evaluation (5 minutes)

➡SLIDE #21

Congratulate learners on their participation in the class. Thank them for attending and ask them to fill out the evaluation form and leave it on a table or in a large envelope you provide. If you will be conducting other trainings at a specific future time, announce that now and encourage learners to attend.

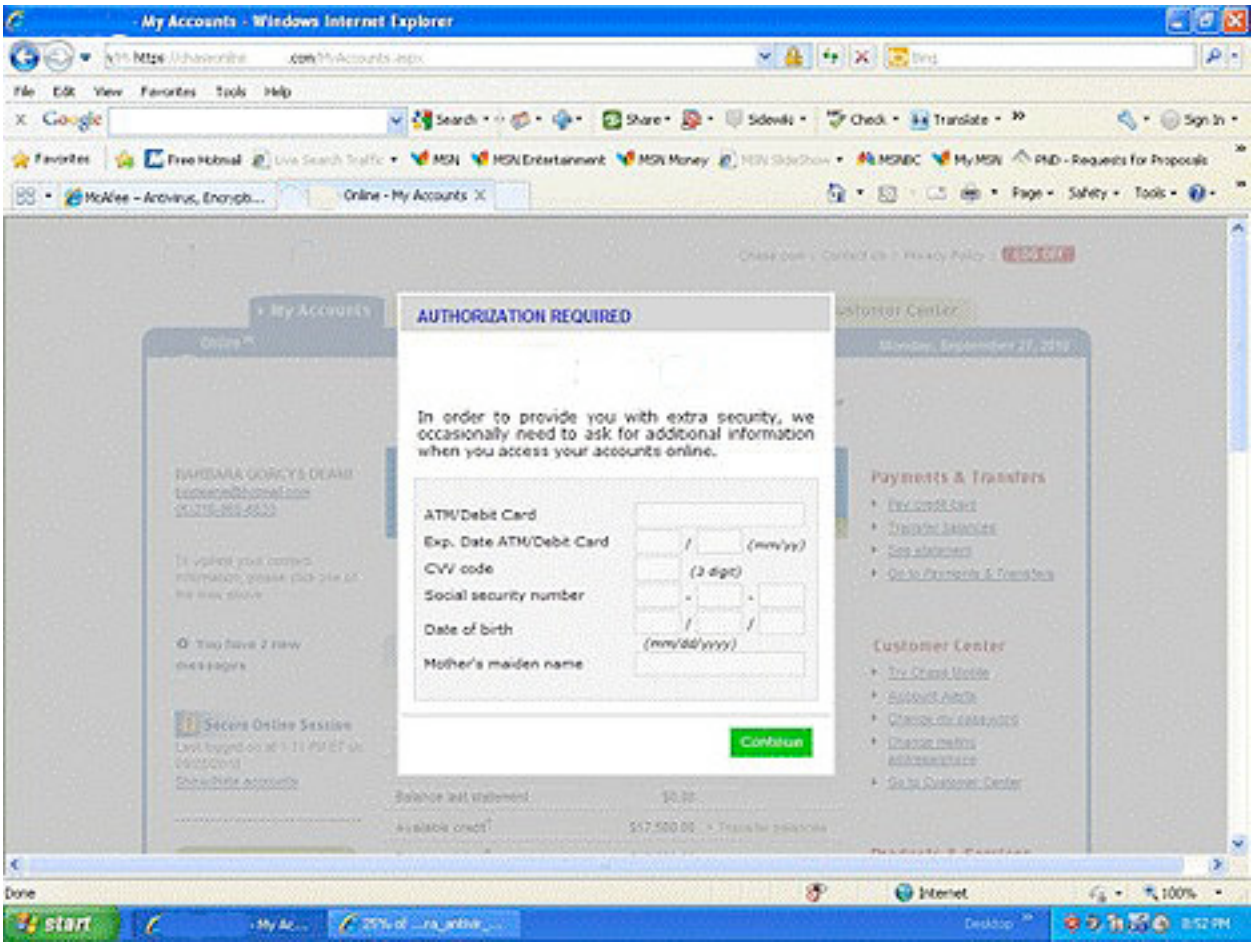
Activity: *What's 'Phish-y' About This?*

In the sample messages and websites below, circle any "red flags"—those things that might tip you off that the source is phishing for personal information. Be prepared to discuss your observations.

1) Phone call to hotel guest in room at 4:30 a.m.

"This is the front desk calling. I'm sorry to bother you but our computer system crashed and we lost all of the credit card information for our registered guests. The auditing department requires us to re-enter all our guests' payment information into the system before the start of the business day. Please give me your credit card information and we will renew your reservation."

2) Pop-up box (appears upon landing on website after clicking a link in an email message)



3) SMS text message

From: yourbank@mail.tmail.com//YourBank
debit card cancellation alert. call 212-444-4444

4) Website you land on after clicking a link in an email message

http://cgi6-secured/irsService/connection_mysql/taxaccounts.irs.com

Tax Refund Claim Form
To claim your refund, please verify your identity and mailing address below.

Name _____ _____

Address _____ Social Security # _____

Accessibility | Appeal a Tax Dispute | Careers | Freedom of Information Act | IRS Privacy Policy
©2009. IRS.gov | Internal Revenue Service | United States Department of the Treasury

5) Email message

From: no_reply@emailonline.friendly-bank.com
Subject: Account Status

Dear Friendly Bank Online[SM] Customer,

Due to recent activity on your account, we have issued the following security requirements. For your security, we have temporarily prevented access to your account. Friendly Bank safeguards your account when there is a possibility that someone other than you tried to sign on. You may be getting this message because you signed in from a different location or device. If this is the case, your access may be restored when you return to your normal sign on method. For immediate access, you are required to follow the intruction below to confirm your account in order to secure your personal account informations.

Click To Confirm Your Account

Samuel Smith
Chief Marketing Officer
Friendly Bank CardMember Services

6) Text message

recent security check requires you to re-activate your paypal account now
www.reactivatepaypal.com

7) Phone call

“I’m calling regarding your credit card. We are offering our customers the opportunity to lower their interest rate today only. Once you confirm your credit card number and expiration date, we will reduce the interest rate by 5%. You will see the reduction on your next statement.”

Key to *What's 'Phish-y' About This?* Activity

1. True story: Once the scammers figured out how to call individual rooms in a hotel, they simply dialed one after another in their search for victims. They called in the middle of the night to find more people in their rooms and to catch them while they were groggy and, perhaps, not thinking so clearly. They also knew that they would be less likely to go to the front desk to confirm the story. A hotel will *not* call a guest in the middle of the night unless it truly is an emergency. Also, major hotels are sure to have backup of all transactions on a main server, making it unnecessary to ask every guest to re-register their credit card. A guest receiving a call like this should hang up and call the front desk directly, or tell the caller that s/he will stop by the front desk with the credit card in the morning.
2. Scammers aren't just building bogus websites, they're making them fancy enough to include popup boxes that ask for your personal information. To avoid landing on a bogus website, always type in the URL (Web address) yourself rather than clicking on a link. Check that you've typed in the address correctly, since many scammers build websites with URLs that reverse a couple of letters, to take advantage of typing errors. Better yet, use a bookmark so you don't risk mistyping the address. A legitimate financial institution will never ask for this kind of personal data (Social Security number, mother's maiden name, account number, CVV security code, expiration date, and birth date) on its website.
3. This "From" address looks suspicious: An email address at mail.tmail.com does not appear to be a standard "YourBank" address despite the appearance of the name twice, once before the @ sign and once at the end. The message itself is cryptic, and there is no punctuation—misspellings, awkward language, incorrect or missing punctuation and strange formatting are all signs of fraudulent communications. The number leads to a fake call center (one scammer waiting for the phone to ring) where the "representative" will ask for your personal information, such as account number and password or Social Security number. If you get a message like this and you are concerned that it may be a legitimate alert, ignore the number, email address or link in the text message and contact the bank directly.
4. The first clue that this is not the official IRS site is that the URL doesn't begin with the real IRS homepage address (www.irs.gov). In this case, the difference is obvious, but in many cases, the scammers use a URL that closely resembles the legitimate Web address for the site they are mimicking—like www. statescredtiunion.org instead of www.statescreditunion.org, or www.charlesschwab.com instead of www.schwab.com, or www.irs.us.gov instead of www.irs.gov. Phishing attempts always ask for one or more sensitive pieces of information that a legitimate financial institution or business would never ask for online or by phone, email or text message. There is also usually a promise of money (a tax refund in this case) or a consequence (such as you account being closed) that instills urgency and requires an immediate response. Scammers copy the logos, images, fonts and formatting straight from the sites they are mimicking, so don't assume that just because the company's logo or a copyright (at the bottom of the page) appears that the site is legitimate. In this case, a consumer should either ignore the email that included the link to this site, or , if s/he were concerned about missing out on a refund, contact the IRS directly through contact information found at the real IRS site: www.irs.gov.
5. This email contains all the phishing red flags: an email address that has "friendly-bank" in it instead of the bank's true URL ("friendlybank"), a threat that account access will denied if you don't respond immediately, a link to a site that will undoubtedly request your personal data, and numerous typos ("intruction" instead of "instruction," "informations" instead of "information," US in the salutation but U.S. in the body of the email, and "CardMember" instead of "Cardmember"). And why would the Chief Marketing Officer be the one contacting

customers about their account status? Again, ignore the email entirely, or contact the bank directly to inquire about the communication.

6. Again, there is no capitalization or punctuation—unlikely in a legitimate communication from such a large company—and there is a requirement for immediate action (to avoid your account being closed). Also, the Web address appears to be bogus despite the appearance of "paypal" in the URL. In cases such as this, either ignore the text (or email) or contact the company directly using a known, legitimate phone number or Web address.
7. A legitimate financial institution will never call and ask you to provide personal data. If you're concerned you might be losing out on a great deal, hang up and call the number on the back of your card.

Additional tips:

- A link may actually appear correct (such as http://www.friendlybank.com) but be coded to lead to an entirely different URL. So always check not only that the link itself looks correct but also that the URL that appears in the browser address bar matches and is also correct.
- Any email purporting to be from a financial institution or other legitimate business that requests your personal information should be considered phony and brought to the attention of the business it claims to be from.
- While a phishing email can come from any source, statistics show that financial institutions, eBay, PayPal and the IRS are some of the identities most widely used by scammers.
- For mobile banking, get your "app" directly from the institution (available on its website) if you have the option. (There were some instances of phishing apps that temporarily appeared in at least one of the online app stores.) To avoid a mobile banking scam, it's best to disregard all messages, even if you believe them to be from your bank. Simply contact your bank as soon as possible—using a known valid email address, phone number, URL or short code—and they can tell you if any messages have been sent or if there is a problem with your account.

Activity: *Mobile Banking and Payment Safety*

Write the correct word or phrase to clarify each statement.

1. You should do this before selling, donating or disposing of your mobile device.

2. It is safest to use one of these when shopping online.

3. Set your mobile device to do this automatically when it's not being used.

4. Delete old ones of these so that they are not accessible if your phone is lost or stolen.

5. Make sure the financial institution offers this, which guarantees you won't be responsible for unauthorized transactions.

6. A strong one of these protects your personal information from being shared with third parties.

7. Using one of these allows you to avoid entering your credit card information every time you make a payment using your mobile device.

8. It's important to do this when you're finished using a financial app.

9. This type of Wi-Fi can leave your information vulnerable when shopping or banking by mobile device or computer.

10. If you receive a text or email message from your financial institution asking for your password, PIN, Social Security number or other sensitive information, it's best to do this.

11. These types of communication are not typically encrypted, so it's best not to send sensitive information using them.

12. Special software can help you do this if your phone is lost or stolen.

13. A strong password should be this long.

14. Before downloading an app from an unknown source, do this.

15. Add your bank's short code to your phone's contact list to know if one of these is actually from your bank and not a scammer.

16. Do this to avoid landing on a fraudulent site because you mistyped the bank's Web address.

Key to *Mobile Banking and Payment Safety* Activity

1. You should "*erase your hard drive completely and permanently"* before selling, donating or disposing of your mobile device. (erase your hard drive completely and permanently)

2. It is safest to use "*a credit card*" when shopping online. (a credit card)

3. Set your mobile device to "*lock*" automatically when it's not being used. (lock)

4. Delete old "*transaction text and email messages*" so that they are not accessible if your phone is lost or stolen. (transaction text and email messages)

5. Make sure the financial institution offers "*a zero-liability policy,*" which guarantees you won't be responsible for unauthorized transactions. (a zero-liability policy)

6. A strong "*privacy policy*" protects your personal information from being shared with third parties. (privacy policy)

7. Using "*a digital wallet or Internet payment service*" allows you to avoid entering your credit card information every time you make a payment using your mobile device. (a digital wallet or Internet payment service)

8. It's important to "*log out and close the app*" when you're finished using a financial app. (log out and close the app)

9. "*Public, non-password-protected*" Wi-Fi can leave your information vulnerable when shopping or banking by mobile device or computer. (public, non-password-protected)

10. If you receive a text or email message from your financial institution asking for your password, PIN, Social Security number or other sensitive information, it's best to "*ignore or delete it and contact the institution directly.*" (ignore or delete it and contact the institution directly)

11. "*Email and instant messaging (IM)*" are not typically encrypted, so it's best not to send sensitive information using them. (email and instant messaging/IM)

12. Special software can help you "*locate the device or remotely "wipe" the data*" if your phone is lost or stolen. (locate the device or remotely "wipe" the data)

13. A strong password should be "*at least eight characters, combining uppercase and lowercase letters, numbers and symbols*." (at least eight characters, combining uppercase and lowercase letters, numbers and symbols)

14. Before downloading an app from an unknown source, "*search online for reviews and user feedback*." (search online for reviews and user feedback)

15. Add your bank's short code to your phone's contact list to know if "a text, or SMS, message" is actually from your bank and not a scammer. (a text, or SMS, message)

16. "*Bookmark your bank's website*" to avoid landing on a fraudulent site because you mistyped the bank's Web address. (bookmark your bank's website)

Training Evaluation: *Your Digital Dollars*

Date and Location of Training:_____

Please help us improve future presentations by giving us your opinion of today's class. Circle the response that best reflects your feelings about each statement:

1. I have a better understanding of how online and mobile banking and payments work.

Strongly agree Agree Disagree Strongly disagree

2. I understand the benefits and risks associated with digital transactions.

Strongly agree Agree Disagree Strongly disagree

3. I know what steps to take and what tools to use to protect my personal information, device, data and accounts and to make every transaction more secure.

Strongly agree Agree Disagree Strongly disagree

4. I know where to go for more information and assistance on this subject.

Strongly agree Agree Disagree Strongly disagree

5. I can use what I learned today to make improvements in my life.

Strongly agree Agree Disagree Strongly disagree

6. The instructor was well informed.

Strongly agree Agree Disagree Strongly disagree

7. The materials I received are easy to read and understand.

Strongly agree Agree Disagree Strongly disagree

8. I would like to attend another class like this.

Strongly agree Agree Disagree Strongly disagree

Please let us know how we could improve future trainings (use back, if necessary):

_____

_____

_____

_____

_____

Thank you for attending!

Your Digital Dollars

Online and mobile banking and payments

Financial education from Consumer Action and Visa Inc.

Online Banking

- Check your balance
- View account activity
- Search for transactions
- View canceled checks
- Transfer money between accounts
- Pay bills
- View account terms
- Set/manage alerts, stop payment, order checks
- Contact customer service

Who offers online banking?

- All major financial institutions:
  - **Banks**
  - **Credit unions**
  - **Lenders**
  - **Investment companies**
- Many smaller financial institutions
- Some banks offer ONLY online account access

The Online Banking Process

- Visit the institution's website
- Log into the system by entering your username or email address and your password
- Click on the account you want to access
- Choose what you want to do with that account
- Sign out (log off) to end your online banking session

Your Digital Dollars

Online Banking Benefits

- Convenience—24/7 access from home, office, etc.
- Fewer—or no—trips into the branch or to an ATM if you use direct deposit and get cash while shopping
- No stamps or trips to the mailbox if you pay your bills online
- No more waiting for the monthly statement to get account information
- Lower cost: fewer checks to buy and low—or no–account fees on “e-accounts”
- Environmentally friendly—no paper, no fuel

Your Digital Dollars

Mobile Banking

- Capabilities depend on device, wireless service, and the institution's technology
- Typically offered by the same financial institutions that offer online banking
- May have to complete the enrollment and setup process on a computer first

Your Digital Dollars

Types of Mobile Banking

- Text (SMS)
  - **Limited capabilities**
  - **Any phone that supports texting**
- Web browser
  - **Same as online banking, but by mobile device**
  - **Requires Web-enabled device and data service plan**
- App (application)
  - **Specially designed program you download/install**
  - **May even be able to deposit checks by photo!**
  - **Requires advanced device w/Wi-Fi or data service**

Your Digital Dollars

Mobile Payments

- Mobile Web payments
  - **Via app or Web browser on your mobile device**
- Mobile text (SMS) payments
- Direct mobile billing
- Mobile peer-to-peer (P2P) payments
- Mobile point-of-sale (POS/proximity) payments

Digital Banking & Payment Review

- online banking
- text (SMS) banking
- mobile app banking
- mobile Web banking payments
- mobile Web payments
- mobile text payments
- direct mobile billing
- mobile P2P payments
- POS/proximity

What to Know About Digital Banking & Payments

- Possible to lose account access temporarily
- Bill payments could arrive late
- Could lose your mobile device
- Potential exposure of sensitive data over unsecured wireless network
- Possible unauthorized access to accounts or data
- Malware, phishing and other scams
- Your info could be sold or used for marketing
- Cost of wireless service

Your Digital Dollars

ACTIVITY:
What's 'Phish-y' About This?

Carefully examine each communication. Identify which part or parts tip you off that it's a phishing attempt and not a legitimate message from a financial institution.

Did you know…

…that your employer may have the right to access the information stored on any computer, phone or other mobile device it provides for you?

The best way to make sure your personal communications remain private is to use a personal (non-work) computer or device.

Protecting Your Mobile Device & Data

- Guard your device like you would your wallet
- Delete old transaction messages
- Don’t save banking info (passwords, acct numbers, etc.) in your phone’s notepad
- Password-protect your device (“lock” it)
- Use software for locating your device or deleting its data remotely
- Contact your carrier immediately if phone is lost
- Erase the hard drive before selling, donating or disposing of a mobile device (or a computer)

Online Banking Precautions

- Make sure institution is legitimate
- Verify that it's FDIC- or NCUA-insured
- Know how long deposits take to clear
- Know how long it takes for bills to get paid
- Know the institution's policies
- Monitor the activity on your accounts regularly—even weekly or daily
- Know cost of mobile banking (wireless service)
- Avoid banking using public or unencrypted Wi-Fi

Vetting Businesses

- Legitimacy, trustworthiness
- Receipt
- Reasonable return policy
- Zero-liability policy
- Encryption
- Extra security features
- Strong privacy policy

Avoiding Scams, Fraud & Malware

- Don’t respond to phone, text or email requests for info (phishing)
- Avoid landing on a spoofed website
- Only patronize trusted sites and sources
- Trust your instincts
- Take advantage of spam and phishing filters
- Take advantage of browser capabilities
- Guard against malware

Your Digital Dollars

Guarding Your Data

- Create strong passwords
- Don’t share logon info
- Log out and close apps and browser windows
- Turn off Bluetooth devices and lock your phone
- Don’t send sensitive data via email or IM
- Lock your home wireless network
- Avoid shopping or banking in a public Wi-Fi hotspot
- Use a digital wallet
- Use a firewall
- Don’t open files, messages or attachments from unknown sources
- Reveal only what is necessary
- Manage your cookies

ACTIVITY:
Mobile Banking and Payment Safety

- Write the correct word or phrase to clarify each statement.

  Example: You should keep this until you receive, and are satisfied with, your purchase.

  Answer: your receipt

Your Digital Dollars

Assistance

- Financial institution's customer service or online/mobile banking technical support departments
- App vendor or developer
- Merchant/seller
- Credit card issuer
- Internet payment service
- Wireless service provider

Learn More!

- OnGuard Online (www.onguardonline.gov)
- Privacy Rights Clearinghouse (www.privacyrights.org)
- Federal Trade Commission (www.ftc.gov)
- FDIC (www.fdic.gov/bank/individual/online/safe.html)
- NCUA (ncua.gov)
- Microsoft Safety & Security Center (www.microsoft.com/security)
- Visa's Practical Money Skills (www.practicalmoneyskills.com)
- Visa's Security Sense (www.visasecuritysense.com)

Congratulations!

You've completed the Digital Dollars training!

Consumer Action
www.consumer-action.org
415-777-9648 / 213-624-4631
outreach@consumer-action.org

bank's contact number or short code in your address book so you'll see its name when you get a legitimate email or text message. And don't respond to text, email or other requests for your password or other private information, even if the sender claims to be someone you do business with.

Avoid landing on a spoofed website—a copy of a legitimate site designed to lure you into revealing your password and other sensitive information—by bookmarking your bank's website while on the legitimate site. (You'll avoid the possibility of mistyping the Web address, or URL.) Don't go to the site by clicking a link in an email or text message.

Download apps only from trusted sources. If the source is unknown, do an online search for reviews and user feedback to find out if others have had problems with the app. (Lookout Mobile Security (www.mylookout.com/about), a free app for Blackberry and Android phones, checks apps for malware, spyware and viruses.) Before using a new app, look into its policy regarding disputed or unauthorized transactions.

Use your wireless carrier's network rather than public (non-passworded) Wi-Fi for shopping or banking. Check for "https" instead of just "http" in the Web browser address bar, which indicates the site is secure and encrypted.

Confirm before making a payment or purchase that you will get a receipt. Keep your receipt until you receive, and are satisfied with, your purchase.

Monitor the activity on your accounts regularly—even weekly or daily. You'll detect fraud sooner rather than later. And, in most cases, you must report unauthorized account activity within a certain time period (say, within 60 days of when the transaction posted) to be protected by a zero liability guarantee. Your wireless carrier and other payment processors all have policies for disputing unauthorized charges to your account, but not all companies offer zero liability. Generally speaking, you'll get the strongest liability protection with the fewest hassles when you use a credit or debit card with a zero liability policy.

Know how long it takes for your transactions to be processed so that you correctly time your payment requests, deposits and other activity.

Contact your wireless provider immediately if you lose your phone, to suspend your service. Then log on to your financial accounts on a computer and deactivate text banking and change your passwords. (Call your bank if you need help.)

Many of the practices for safe mobile banking are the same as those recommended for secure online banking. *(Learn more in the "Digital Dollars" companion brochure "Banking online safely," available at www.consumer-action.org.)*

Though it's not an issue of safety, be aware that mobile banking activity may cost you money in higher wireless service bills. If so, consider online banking from your home computer or inquire about other service plans that better accommodate your usage.

Assistance

Whether you're already a mobile banking customer or just getting started, you can contact your financial institution's customer service department directly for guidance. Likewise, contact the app vendor or the merchant regarding any mobile payment questions or issues.

If you're dissatisfied with a purchase, try first to resolve the issue directly with the seller. If you aren't able to come to an agreement and you want to dispute a payment, contact the credit card company or financial institution that issued the card you used to make the purchase.

If your payment was processed through an intermediary, such as an Internet payment service account or your wireless service provider, follow that company's instructions for filing a dispute.

Learn more

Learn more about staying safe while using mobile and Web-enabled devices:

OnGuard Online: ***www.onguardonline.gov***

The U.S. federal government and the technology industry provide information and tips for online safety and security.

Privacy Rights Clearinghouse: ***www.privacyrights.org***

The nonprofit Privacy Rights Clearinghouse offers a library of information, from tips for protecting your privacy online to how to shop safely on the Internet.

Consumer Action

www.consumer-action.org

Consumer advice and referral hotline:
hotline@consumer-action.org or 415-777-9635
Chinese, English and Spanish spoken

Consumer Action created the Digital Dollar series with funding from Visa Inc.

VISA

consumer action
Education and advocacy since 1971

Visit Visa's financial education program, Practical Money Skills, at: *www.practicalmoneyskills.com*

Your Digital Dollars

Mobile banking and mobile payments

Make financial transactions safely on the go

Financial education from *Consumer Action* and *Visa Inc.*

Check your balance…transfer money…make a purchase—these are just a few of the things you can do on the go with a cellular telephone or other mobile device.

There are a lot of benefits to being able to bank or make payments from just about anywhere, but it's important to know how to do these things safely. Understanding the types of transactions that are possible on a mobile device, the potential risks of banking and paying on the go, and how to keep your personal information, money and credit safe can help you get the most out of mobile technology.

What is mobile banking?

Mobile banking allows you to access your financial accounts and conduct transactions wirelessly, using your mobile device. Most major financial institutions, including banks, credit unions, lenders and investment companies, offer mobile banking. Increasingly, smaller financial institutions also offer mobile banking.

What you can do using a mobile device depends on the technology used by the bank, your wireless service plan and the type of phone, smart device, tablet computer or PDA (personal digital assistant) you have. You need a smartphone with data service or Internet access to take advantage of the most advanced mobile banking capabilities. Before you can access accounts on your mobile device, you may be required to complete the enrollment and setup process on a computer.

There are three types of mobile banking that your bank may offer:

- Text, or SMS (short message service)**.** Text banking allows you to get information about your account (such as your balance) and receive information and alerts via text message. It's possible from any cell phone that supports texting, but usually you can't conduct transactions.
- Online banking via mobile device. You log on to your bank account using your mobile device's Web browser, just like you would on a laptop or desktop computer. It enables you to do all the same things you can do with online banking. This requires a Web-enabled device and a data service plan.
- Mobile banking applications. "Apps" are specially designed programs that are downloaded and installed on a smartphone, tablet or PDA. Apps typically are faster to use and easier to navigate on a small screen than a website is, and they allow you to conduct the full range of transactions. (Some banking apps even allow you to make a deposit by taking a picture of the front and back of the check!) To use a mobile banking app, you must have an advanced mobile device with Wi-Fi or a data service plan.

What are mobile payments?

Mobile payments are payments you make using your mobile device, instead of writing a check, handing over cash or pulling out a credit or debit card.

There are many types of mobile payments:

Mobile Web payments allow you to make purchases remotely, when shopping on your mobile device via a downloaded app or your Web browser. The purchase amount typically is charged to a credit or debit card, a pre-registered Internet payment service account or a "digital wallet" (a program that stores your payment and shipping information for Internet and electronic transactions).

Mobile text (SMS) payments allow you to make purchases via text message. This is sometimes called "text to buy." The transaction might be added to your wireless service bill or charged to a pre-registered credit or debit card, Internet payment service account or digital wallet. This type of mobile payment typically is used for small amounts, such as the cost of downloads (ringtones and songs, for example), parking fees, transportation fares and movie tickets, though it is even possible to authorize a payment to family members in another country by text message or buy big-ticket items from certain retailers.

Direct mobile billing (less common) allows you to have purchases added directly to your wireless service bill at checkout if the option is available.

Mobile peer-to-peer (P2P) payments are typically small, informal transactions between two people—for example, paying a handyman or covering part of a dinner bill. The payment may be made using an app or, less common, by touching two smartphones together.

Mobile point-of-sale payments (also known as proximity payments) make it possible to make purchases at the cash register or other point of sale simply by tapping or waving your mobile device close to an electronic reader. This payment option is becoming more widely available as more phone manufacturers and merchants install the necessary chips and chip readers.

What to know

Making purchases and banking by mobile device isn't particularly risky, but that doesn't mean that it's absolutely risk-free. It's important for anyone who uses mobile banking and payment technology to be aware that:

- It's possible to lose access to your accounts if you're outside your wireless service coverage area or your phone battery is dead. Bill payments could be late if you can't get service in time to place the payment request. (This is a great reason to pay bills early whenever possible!)
- It's far more likely that you would lose your mobile device than, say, a desktop computer. A lost phone would not only be inconvenient, it could leave your personal data, account information and purchase ability accessible to someone who finds it. *(See "Safety tips.")*

  TIP: *Anytime you send sensitive information over an unsecured wireless network, it could be exposed.*

- Though not a major issue so far, malware (viruses, spyware and other code designed to steal your information or do harm to your device or data) could hit phones more widely in the future. Antivirus and firewall protection is not yet widely available for mobile devices.
- Mobile banking could cost you money if you pay for service per unit (text message or megabyte of data), if you use more text messages or data than is included in your monthly service plan or if you use your service while roaming outside your carrier's network.

Safety tips

Financial institutions, card issuers, major retailers, payment networks, wireless service providers, etc. work hard to make mobile banking and mobile payments safe and problem-free. Still, there are things you can do yourself to protect your information, accounts and mobile device.

Guard your mobile device like you would your wallet, since it may contain information that someone could use to make purchases or access your accounts. Don't lend your phone to anyone you don't know and trust. Find out if there is a way to delete the device's contents remotely if it's lost or stolen. (There are many software products available that help owners locate missing devices or remotely "wipe" personal data from the phone.)

Create strong passwords for both your device (to turn it on or wake it up from sleep mode) and all your banking and payment apps. They should be at least eight characters long and use a combination of uppercase and lowercase letters, numbers and symbols. Don't share your passwords, personal identification numbers (PINs), usernames or the answers to "password hints" with anyone. Don't use the "Remember me" function or similar options to store passwords or payment information on sites or in apps. Change your password regularly; change it immediately if you think it's been compromised.

Log off and close the browser window or the app when you're finished. Turn off Bluetooth devices that link to your phone when you are not using them. Lock your phone when not in use.

Don't send sensitive information via email or instant message (IM), since these aren't automatically encrypted. Keep your