

WORKSHOP 5

Understanding Debit Cards

A **debit card** looks like a credit card but works like an electronic check by deducting your payment directly from your checking or savings account. If you use a debit card at a retail store, your card runs through a scanner that enables your financial institution to 1) verify electronically that the funds are available and 2) approve the transaction. In addition to making instant payments in stores or online, most debit cards can be used to withdraw cash at ATMs or at most supermarkets when you make a purchase.

Benefits of Debit Cards:

For many people, it is more convenient to carry a small, plastic card instead of a bulky checkbook or a large amount of cash. Using a debit card is easier and faster than writing a check. It's a good way to pay for purchases without having to pay interest, as you would if using a credit card with an outstanding balance. Debit cards take the money directly out of your bank account, so there is no worry of racking up credit when using them.

FAQs about Debit Cards

What kinds of costs are associated with debit cards?

There may be fees for using your debit card. As with other bank products, your financial institution must provide disclosures explaining the possible fees associated with a debit card. Be sure to read the disclosures to avoid an unexpected fee.

- Some banks charge a fee if you enter a PIN (Personal Identification Number) to conduct a transaction instead of signing your name.
- You may trigger a fee if you overdraw your account using your debit card, just as you would if you "bounced" a check.
- There could be a charge if you use your debit card at an ATM that is not operated by your financial institution.

Some debit cards come with rewards or other incentives for using them. How can I know which one is a good deal?

As with similar financial products, rewards-linked debit cards are designed to encourage people to use a certain bank and its services. Similar to many credit cards, some debit cards offer rewards, such as cash back, giving you the opportunity to earn points for your purchases. Before opening a new account or changing banks to get a different perk, study the fine print. Begin by reading the disclosures that explain the account terms and fees to understand the potential benefits as well as the costs, such as fees for overdrawing your account (discussed below).

How is it possible to overdraw my account if my bank or bank network must approve a debit card transaction?

Because debit card payments are electronic, they are deducted from your account more quickly than when using a paper check. Oftentimes, a debit card purchase is posted within 24 hours instead of a few days, as may be the case with a paper check. This means there is less time to make a deposit to cover a purchase, if necessary.

In addition, even if a transaction was approved, you may overdraw your account because the bank won't know what other withdrawals you have made that day until it settles all transactions later that day. Or, suppose you don't realize you have only \$100 in your bank account and you want to use your debit card to buy a \$200 item. Depending on the terms of your account, the bank might approve the \$200 purchase as a convenience, but it also might assess an overdraft fee for that transaction and subsequent ones until you make a sufficient deposit.

Note: If your debit card is linked to your savings account, you can transfer money to your checking account when funds get low to avoid these fees. Mobile banking apps also make it easy to check your account balance for sufficient funds before making a purchase.

If I use a debit card to make a purchase can the merchant put a temporary "block" or "hold" on other funds in my account?

Yes, in certain circumstances merchants can take these steps as protection against fraud, errors, or other losses. For example, a hotel might put a hold on a certain amount when you use a debit or credit card to reserve a room. Another example is when you use your debit card at the gas

pump. Typically, the gas station will create two transactions: the first to get approval from your bank for an estimated purchase amount (like \$50) when you swipe your card before pumping gas, and the second for the actual charges when you're done. Until the first (\$50) transaction is cancelled by the bank, usually within 48 hours, you won't have access to that amount in your account.

Because a debit card transaction is processed so fast, is it possible to order a "stop payment" or obtain a refund if I later discover a problem with the merchandise?

It depends. Because funds are deducted from your account very quickly, don't expect to have the option to stop payment or obtain a refund. If the transaction cannot be cancelled, you may be able to work out other arrangements with the store. For example, if you return an item to a merchant and you're not able to get a refund, you instead may qualify for store credit or a gift card.

Consumer protections are stronger for credit cards than debit cards, so if you are concerned that merchandise may be damaged or not what you expected, you may consider using a credit card for those types of purchases. The Fair Credit Billing Act (which only applies to credit cards) gives you the ability, under certain circumstances, to withhold payment on defective goods until the problem has been corrected.

Sometimes I'm asked to enter a PIN to approve a debit card transaction, other times I can sign my name. Does it matter?

It could matter. If you use a PIN at a merchant's sales counter, you also may be able to get cash back, and that can save you a trip to the ATM. However, be aware that some financial institutions charge consumers a fee for a PIN-based transaction. There also may be differences in how quickly the transaction is posted to your account, depending on how your bank processes PIN vs. signature debits.

If you would rather sign for a debit card transaction, you can generally swipe your card through the reader and choose "credit" (even though you are authorizing a debit withdrawal from your account, not a credit card transaction). To use your PIN instead of signing, select "debit."

Debit Card Safety

Debit card fraud is a common form of identity fraud that can affect anyone. It is important to protect your debit card as well as your account number, expiration date, security code (the three-digit number on the back of your card), and your PIN. Identity theft can occur even if you don't lose or misplace your debit card. Someone who has learned your account number, security code, and PIN can use that information to access your account, withdraw funds, or create counterfeit cards. While in many cases you are not responsible for unauthorized transactions, it can be a hassle to resolve the situation.

Tips to Avoid The Risk of Debit Card Fraud:

- Never write your PIN on or near your card. Memorize it instead.
- Don't give out bank account information over the phone or the Internet unless you have initiated the contact or you know the person is who they claim to be. Beware of deceptive calls or emails from individuals claiming to be from your bank asking you to "verify" your account information. A true bank representative would **never** ask for your PIN because your bank already has that information.
- Don't share your PIN, security code or other account information with friends or relatives who aren't co-owners of your account. Never reveal this information to new friends you meet over the Internet. Common scams occur with a false job offer or Internet friendship or romance, in which the victim is asked to transfer money to the perpetrator.
- Take precautions at the checkout counter, ATM, and gas pump. Always stand so that no one can see the keypad where you enter your PIN. At retail establishments, it's best to use do-it-yourself scanners. If you give your card to a clerk, make sure they don't run your card through two scanners instead of one. The second scanner could be capturing your account information to make a counterfeit card. In general, be alert for suspicious-looking devices that may be used to "skim" information from your card.
- If you use your debit card to shop online, consider extra precautions with your personal computer. Use similar precautions with Internet and mobile banking. Experts advise installing virus and spyware protection to stop thieves from secretly installing malicious software that can be used to spy on your computer and obtain account information.
- Look at your bank statements as soon as they arrive. Or better yet, review your account each week. Promptly report any discrepancy, such as a missing payment or an unauthorized transaction, to your bank. Your quick attention to the problem may help limit your liability and give law enforcement authorities a head start on stopping the thief.

Federal Protections for Consumer Debit Cards: The federal Electronic Fund Transfer Act (EFTA) protects you from errors, loss, or theft of your debit card. However, unlike the Truth in Lending Act protections for credit cards, which cap a consumer's liability for unauthorized transactions at \$50, the law limits liability to \$50 if the cardholder notifies the bank within two business days after discovering the theft. If you do not notify your bank within those two days, you could lose up to \$500. If you receive a bank statement that includes an unauthorized debit-card withdrawal and you wait more than 60 days to alert your bank, you could be liable for any amount of the transactions made after that 60-day period. The good news is that many banks do not hold a consumer responsible for unauthorized transactions if they notify the institution in a timely fashion. However, remember that with a debit card, the money tapped by the thief has already been taken out of your account.

Under the EFTA, a bank has 10 business days to investigate the matter (20 business days if your account is new) and report back to you with its results. If the bank needs additional time, it may, under certain circumstances, temporarily give you some or all of the disputed amount until it finishes its investigation. Generally, a bank is allowed up to 45 days of additional investigation time.⁶⁰

How to Use an ATM

While machines vary slightly, most ATMs have similar characteristics which makes them fairly easy to navigate. The basic steps are generally the same:

1. Either insert your card into the slot or swipe it, depending on the machine.
2. Enter your personal identification number (PIN).
3. If you are using a machine unaffiliated with your bank, you may be asked if you accept the charge to use the machine (usually between \$1.00 and \$3.00). If you do not want these charges to be taken from your account, you can cancel at this time.
4. Choose a transaction.
 - a. If you want to withdraw money, select this option. Most machines dispense money only in increments of \$20 (i.e. \$20; \$40; \$60 etc.). Most banks have a limit of what you can withdraw from an ATM in a single day, usually \$300 Or \$400. If you want more than your limit, you'll have to go into your bank and speak with a teller.

⁶⁰ "Beware of ATM, Debit and Credit Card 'Skimming' Schemes." *FDIC Consumer News*, 2018. <https://www.fdic.gov/consumers/consumer/news/cnwin18/cardskimming.html>

- b. If you want to make a deposit, select this option. Some machines require a deposit slip and your cash and/or checks to be placed in an envelope. Some machines do not allow you to make deposits in cash.
- 5. You will be asked if you want a receipt. Click “Yes” or “No.”
- 6. When you are finished with your transaction(s), be sure to take your card, your money (if you made a withdrawal), and your receipt (if you requested one).⁶¹

Note: It's a good idea to find out which machines are affiliated with your bank (to avoid charges) and what the withdrawal limits are for those ATMs.

What is an ATM Skimmer?

ATM skimming is a form of credit or debit card fraud in which scammers rig ATMs with hidden recording devices to steal a person’s card information. A skimmer is a card reader that is disguised to look like part of the ATM. The skimmer collects a person’s card numbers and PIN, which theives can use to make purchases, withdraw cash, or produce fake cards. Some methods of ATM skimming include an overlay on the keypad that captures a person’s PIN as they enter it; an overlay on the card insertion slot that records the data on the card’s magnetic strip; or tiny cameras that record a person typing in their PIN.⁶² Skimmers are becoming more advanced as technology advances. However, there are ways to protect yourself from ATM skimming, such as:

- Check the PIN keypad and the slot where you insert your card, which are usually bulkier when a skimmer is in place.
- Check for tape or glue residue on the ATM and wiggle the card slot or keypad to check for loose-fitting attachments. Don’t use ATMs that have damaged or loose parts.
- Use debit and credit cards with chip technology, which is more secure.
- Use your smartphone instead of a physical card, such as through your bank’s mobile app or Google Pay, Apple Pay, Samsung Pay or PayPal.
- Run your debit card as a credit card transaction so you won’t need to enter your PIN.
- Review your debit and credit card transactions at least once a week to catch any form of fraud early on. Sign up for account alerts.⁶³

⁶¹ Original material from Peerlink National Technical Assistance Center.

⁶² Libby Wells. “What is ATM skimming and how do you protect yourself?” *Bankrate*, Oct. 19, 2020. <https://www.bankrate.com/banking/what-is-atm-skimming/>

⁶³ “How to Spot an ATM Skimmer.” *Northwest Community Credit Union*, 2022. <https://www.nwcu.com/learn/how-spot-atm-skimmer>

ATM Safety Tips:⁶⁴

Below are a few practices for using an ATM safely:

- Always pay close attention to the ATM and your surroundings. Don't select an ATM at the corner of a building – corners create a blind spot. Use an ATM located near the center of a building.
- Do your automated banking in a public, well-lit location not blocked by shrubbery. Bring another person with you, if possible.
- Maintain an awareness of your surroundings throughout the entire transaction. Be wary of people trying to help you with ATM transactions. Be aware of anyone sitting in a parked car nearby. When leaving an ATM make sure you are not being followed. If you are, drive immediately to a police, fire station or business or to a crowded, well-lit location.
- Do not use an ATM that appears unusual-looking or offers options with which you are not familiar or comfortable.
- Do not allow people to look over your shoulder as you enter your PIN.
- Memorize your PIN, never write it on the back of your card. Do not re-enter your PIN if the ATM eats your card – contact a bank official instead.
- Do not wear expensive jewelry or take other valuables to the ATM. This is an added incentive to the assailant.
- Never count cash at the machine or in public. Wait until you are in your car or another secure place.
- When using a drive-up ATM, keep your engine running, your doors locked and leave enough room to maneuver between your car and the one ahead of you in line.
- Maintain a supply of deposit envelopes at home or in your car. Prepare all transaction paperwork prior to your arrival at the ATM. This will minimize the amount of time spent at the machine.
- Closely monitor your bank statements, as well as your balances, and immediately report any problems to your bank.
- If you are involved in a confrontation with an assailant who demands your money, the best thing to do is **comply**.

⁶⁴ "ATM Safety Tips." *American Bankers Association*, 2021.

<https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/atm-safety-tips#>

Online Banking

Today, many people use their computers and smartphones as a way to communicate with the world and do business. There are a wide variety of applications that have been created to assist with banking, budgeting, sending money to other individuals, and investing. When downloading and using these apps, make sure they are *secure* and *certified*. Technological advancements have made these convenient banking and money sharing apps possible, but have also made Internet hacking and scams more efficient.

There are a number of apps made to assist individuals with their financial needs. Depending on its particular service, these apps may allow you to:

- Check your balance
- View all of your transactions (all your purchases for a particular time period)
- Pay bills
- Open a new account
- Deposit checks
- Transfer money within your personal accounts (such as from savings to checking)
- Send and receive money
- Invest your money
- Budget

This is not an exhaustive list, as there are numerous apps that can be used for online banking and personal finance. Your financial institution will most likely have their own website and app available to support your online banking needs, as well as a bank representative who can help you with learning how to use these services. Check in with your bank if you have questions or concerns about their banking apps.⁶⁵

⁶⁵ Original material from Peerlink National Technical Assistance Center.

Virtual Banks

If you don't mind foregoing the teller window, an online or e-bank – such as USAA, Chime, NationWide, Discover Bank, Giant Bank or Alliant Credit Union – may save you money. From the customer's perspective, virtual banks exist entirely on the Internet. They offer nearly the same range of services and adhere to the same federal regulations as a brick-and-mortar bank.

Virtual banks pass the money they save on overhead costs, like buildings and tellers, along to you in the form of higher yields, lower fees, rewards such as cashback, and more generous account thresholds. Many of these online banks provide customers access to free (no fee) ATMs across the country. However, out-of-network ATM fees can apply if there are limited ATMs in your area affiliated with your virtual bank. This is the primary disadvantage of virtual banks.⁶⁶

Advantages of Online Banks:

- **Low fees:** Online banks tend to have lower (or no) monthly maintenance or overdraft fees.
- **Better interest rates:** Deposit accounts at online banks tend to have higher annual percentage yields. For example, the best online savings accounts have APYs around 0.45%, while the national average rate for savings accounts is 0.06%.
- **Convenience:** Unlike your corner bank, online banking sites never close; they're available 24 hours a day, seven days a week, and they're only a click away.
- **Ubiquity:** If you're out of state or even out of the country when a money problem arises, you can log on instantly to your online bank and take care of business, 24/7.
- **Transaction speed:** Online bank sites generally execute and confirm transactions at or quicker than ATM processing speeds.
- **Efficiency:** You can access and manage all of your bank accounts, including IRAs, CDs, even securities, from one secure site.
- **Effectiveness:** Many online banking sites now offer tools such as account aggregation, stock quotes, rate alerts, and portfolio programs to help you manage your assets. Most are compatible with money managing programs such as Quicken and Microsoft Money.

Disadvantages of Online Banks:

- **Start-up may take time:** In order to open an account at a virtual bank, you will likely need to mail in a signature.

⁶⁶ Amber Murakami-Fester. "What is Online Banking? Definition, Pros and Cons. *NerdWallet*, May 25, 2021. <https://www.nerdwallet.com/article/banking/pros-cons-online-only-banking>

- **Cash deposits can be difficult:** Because there are no physical branches to make deposits at, you may have to find a deposit-accepting ATM.
- **Cash withdrawals can be difficult:** Some online banks have limits for how much you can withdraw at an ATM. This can be difficult if you need to make a big purchase in cash.
- **Fewer options:** Some online banks may not offer additional accounts and services, such as CDs, whereas traditional banks tend to often offer a number of services all in one place.
- **Learning curve:** Banking sites can be difficult to navigate at first. Plan to spend some time reading the tutorials in order to become comfortable in your virtual lobby.
- **Bank site changes:** All banks periodically upgrade their online programs and add new features. In some cases, you may have to re-enter your account information.
- **The trust issue:** For many people, the biggest hurdle to online banking is learning to trust it. Did my transaction go through? To be sure, always print the transaction receipt and keep it with your bank records until it shows up on your bank statement.

Money Transfer Applications

Along with online banking, money transfer apps like CASH APP, PayPal, Venmo, and Zelle are becoming more and more common. These apps enable you to pay friends or people you are doing business with directly from your phone instead of through cash or checks. Note that Venmo now taxes small businesses for doing business on their app.

Cash apps are intended to request and send money to and from people whom you know and trust or have interacted with before on a financial level. Most financial institutions enable you to request and transfer funds by linking your bank account to your Venmo or PayPal account. If you are hesitant about the safety of these apps, ask a bank representative at your financial institution.

Investment Applications

Investment applications such as Acorns, RobinHood, E*Trade, or Vanguard enable you to put spare change or additional savings into an investment account that will help your money to grow like a 401(k) or an IRA (these are common retirement accounts, which will be discussed further in Workshop 10). Depending on your financial institution, you may be able to invest funds through your bank's mobile app as well. These apps build and manage portfolios for you, making investment easy and jargon-free.

There are several different types of investment apps. Some are micro-investing apps like Acorns, which automatically invests your spare change into diversified portfolios. There are also "robo-

advisor” apps, like Betterment, that use algorithms to assist users on how to invest their money; and stock trading apps, like RobinHood, that provide commission-free investing and trading.

The major downside to these applications is that they cost a monthly subscription fee, which can often be quite high compared to the returns on your investment you are receiving each month. In this case, sometimes traditional investment companies like Charles Schwab or Vanguard, which both have electronic and low-fee options, may be a better option.⁶⁷

If you are interested in investing, make sure you have enough money to meet your daily needs, as well as emergency savings funds, in case your investment loses money. Investments can be risky and a person or family should reach financial stability and resiliency before investing.

Direct Deposit/ACH payments

ACH stands for “Automated Clearing House” and is a financial network used for electronic payments and money transfers in the United States. Many employers, instead of handing or mailing your paychecks, have switched over to directly depositing money into your account. If your employer deposits money directly into your account or you pay your bills online, ACH payments are most likely occurring.⁶⁸

When you begin a job that prefers direct deposit payments, you will often need to provide your employer with your checking or savings account number and your bank’s routing number. These can be found on a blank check (see Workshop 4) or your account information on your bank’s app or website. Sometimes you will need to request a Direct Deposit/ACH letter from your bank to get this information.

Payments from Social Security⁶⁹

If you qualify for Social Security benefits, you must receive your payments electronically. One way to receive your benefits is through direct deposit. It is a simple, safe, and secure way to get benefits. Contact your bank to help you get set up with direct deposit or sign up through the SSA. The other way to receive your benefits is through an electronic debit card, called the Direct Express card. This card is:

⁶⁷ Julia Glum. “Do Investing Apps Actually Work? Here’s What to Know Before you Commit.” *Money*, Dec. 16, 2019. <https://money.com/investing-apps-pros-cons/>

⁶⁸ “What are ACH Payments and Should I Accept Them?” *Square*, 2021. <https://squareup.com/us/en/townsquare/ach-payments>

⁶⁹ “Get Your Payments Electronically” *Social Security Administration*, Dec. 2020. <https://www.ssa.gov/pubs/EN-05-10073.pdf>

- **Convenient and reliable:** Your money will be automatically loaded onto your card on payment day each month. You will have access to your money at all times.
- **Easy to use:** You can make purchases, pay bills online, get cashback at stores, get cash at an ATM or from bank or credit union tellers; or buy money orders at the post office.
- **Secure.** Similar to a regular debit card, you have a PIN that protects your account. The money in your card account is protected and insured for up to \$250,000 by the FDIC.
- **Funds are protected from creditors:** Federal law makes it illegal for a creditor to seize your Social Security benefits. This includes benefits you get on a debit card.
- **It's free to use the card:** There are no sign-up or monthly fees, though some optional services do charge fees.

Visit <https://www.ssa.gov/deposit/howtosign.htm> to sign up for Direct Deposit or Direct Express.

Automatic Bill Payments

Automatic bill pay can be a convenient way to pay most of your monthly bills. The money is automatically taken from your checking account on the same day every month (if the date lands on a holiday or a Sunday, it is usually taken out the next business day). It is relatively easy to set up by phone or through a company's website. You will need the name of your bank, your checking account or debit/credit card number, and your account number that appears on your bills.

What to consider before deciding to use automatic bill pay:

- Check the due dates and make sure the money is in your account. Can you guarantee your account will have enough money for each bill every month when it's due? You may incur fees from your bank *and* the company if your account has insufficient funds.
- Check your statements for discrepancies in your bills. It's easy to overlook mistakes if the bill is taken care of automatically.
- Keep records. If you only get receipts through emails, flag or print them.
- To protect your identity with various accounts, don't use easy-to-guess passwords. Make sure your computer has up-to-date anti-virus software installed.⁷⁰

⁷⁰ Original material from Peerlink National Technical Assistance Center.

Safe Banking over the Internet

The Internet offers the potential for safe, convenient new ways to shop for financial services and conduct your banking business. Whether you are selecting a traditional bank or an online bank, it is important to make sure that the bank is *legitimate* and that your deposits are *federally insured*.

When using online banking systems:

1. Keep your personal information private and secure
2. Understand your rights as a consumer; and
3. Learn where to go for more assistance from banking regulators.

Tips for Safe Internet Banking:

1. Read key information about the bank on its website. Most bank websites have an “About Us” section that describes the institution, where you might find the bank’s history, the official name and address of its headquarters, and information about its FDIC insurance coverage.

2. Protect yourself from fraudulent websites. Watch out for copycat websites that deliberately use a name or web address very similar to that of a real financial institution. These websites try to get your personal information, such as your account number and password. Check if you have typed in the correct web address for your bank before conducting a transaction.

3. Verify the bank’s insurance status. Look for the FDIC logo or the words “Member FDIC” or “FDIC Insured” on their website. You can also check the FDIC’s online database of FDIC-insured institutions. If your bank does not appear on that list, contact the FDIC.

- a. Some bank websites provide links directly to the FDIC’s website to assist you in identifying or verifying the insurance protection of their deposits.
- b. Note that not all banks operating online are insured by the FDIC. Many banks that are not insured are chartered overseas. If you choose one of these banks, know that the FDIC may not insure your deposits, which can be risky. Contact your bank or the FDIC if you are uncertain.
- c. For insurance purposes, be aware that a bank may use different names for its online or traditional services. This does not mean that you are dealing with two separate banks. Talk to your banker if you have questions.

4. For assistance from the FDIC regarding the legitimacy of an institution or the insurance of your deposits, you can call the FDIC's Division of Compliance and Consumer Affairs or send an email through their website. Their website also has an Electronic Deposit Insurance Estimator that can help you determine the amount of your insurance coverage.⁷¹

Note: Only deposits offered by FDIC-insured institutions are protected by the FDIC. Non-deposit investment and insurance products, such as mutual funds, stocks, annuities, and life insurance policies sold online or through the bank itself are not FDIC-insured, are not guaranteed by the bank, and may lose value.

Money Safety

Identity theft: Identity theft occurs when someone uses your personal, sensitive information to either steal from you or pretend to be you. Some forms of identity theft include: using the money in your bank or investment accounts, opening up new lines of credit, using your insurance information, or stealing your tax refund.⁷²

The first step to preventing identity theft is awareness of how and when you use your personal information. By keeping close tabs on your personal information, you can reduce your chances of becoming a victim of identity theft.

Tips to Avoid Identity Theft:

Protect Your Personal Information:

- Memorize your Social Security number and passwords. Do not record your password on papers you carry with you and do not carry your Social Security card or birth certificate with you.
- Do not use your date of birth as your password. Use strong, complex passwords and add an authentication step (such as text message or email verification) to your financial accounts.
- Shred pre-approved credit applications and other financial documents before discarding them.

⁷¹ Federal Deposit Insurance Corporation (FDIC), 2021. <https://www.fdic.gov/>

⁷² Bev O'Shea. "Identity Theft: What It Is, How to Prevent It, Warning Signs and Tips." Aug. 4, 2021. <https://www.nerdwallet.com/article/finance/how-to-prevent-identity-theft>

- Watch your mailbox for stolen mail, which is one of the easiest ways for people to steal your identity.

Review Your Transactions & Statements:

- Order credit reports every year from each of the major credit reporting agencies and thoroughly review them for accuracy.
- Sign up for alerts from your bank, so you can track your transactions and quickly identify any that are suspicious.
- Check your monthly credit card and bank statements for unusual activity.

Practice Internet & Phone Safety:

- Be aware of *phishing* and *spoofing* – spam phone calls and emails from what seems to be a government entity or financial institution asking for sensitive information.
- If you are using a shared computer to check your bank balance or transfer funds, log-out of your account when you are finished to protect your money and information. Do not auto-save passwords.
- Do not download files sent to you by strangers or click on hyperlinks from people you don't know. Be aware of opening attachments in emails or text messages, as they could contain malicious software.
- Don't use public Wi-Fi for sensitive transactions, like banking or online shopping.
- Use a firewall program on your computer.
- Never give personal or financial information over the phone or Internet unless you initiated the contact. Be aware of common phone scams, which can be found here:
<https://www.consumer.ftc.gov/articles/phone-scams>

Take Immediate Action:

- Freeze your credit with the three major credit bureaus if you suspect someone has stolen your information. This stops new lines of credit from being opened.
- Report lost or stolen credit or debit cards *immediately*.

Additional Money Safety Tips⁷³

- Do not carry large amounts of cash in your pocket.
- Be watchful of your surroundings. Be careful not to show money you have on hand (i.e. counting out your cash at an ATM).
- Don't leave money out when you have visitors in your home. Keep only small amounts at home in a safe place.

To report identity theft, go to <https://www.identitytheft.gov/#/>

You may also have to contact your local police department, the Credit Bureaus, the Postal Service, your bank or Credit Card Company, the IRS, or your medical provider depending on the type of theft that occurred.

⁷³ Original material from Peerlink National Technical Assistance Center.

WORKSHOP 5: SUMMARY

In this section, we learned about debit cards: how they work; why people use them; their benefits; and common costs, fees, and incentives associated with them.

We began our discussion of money safety by learning how to prevent debit card fraud. We also learned tips for how to use an ATM safely.

Then, we discussed different online banking options and the pros and cons of virtual banks. We also explored mobile banking and money transfer and investment applications.

We learned about how direct deposit works, and explored the direct deposit and debit options for receiving Social Security benefits.

Next, we learned about automatic bill payments and tips for safe banking over the Internet.

Lastly, we learned additional money safety tips for how to avoid, and respond to, identity theft.

How can the topics I learned in this section be helpful for me?

Topic	N/A	How this will be helpful to me:
Understanding how debit cards work and debit card safety		
How to use an ATM & ATM safety		
Virtual banks & electronic banking		
Banking, money transfer, and investment apps		
Automatic bill paying		
Direct Deposit & the debit system through Social Security		
Money safety and tips to avoid identity theft		



WORKSHOP 6

CREDIT & LOANS

