**Safe Banking**

* **Automatic Payments (Auto Debits):**
* What are Auto Debits?

Automatic payments or “auto debits” are established when you authorize a company or organization to deduct or withdraw funds from your bank account on a regular basis. Some common examples of payments where an auto debit may be used are: mortgage payments, insurance premiums, car payments, utility bills, credit cards, dues, and donations.

* How do you create an auto debit?

There are a number of ways to set up auto debits. Auto debits may be offered or established when you sign a contract, as an option on your billing statement, as an option on your banking institution’s website, through a payment service such as PayPal, or by express permission over the phone. It is important to stress that in order to set up an auto debit, a company or organization must obtain your express permission or authorization. Authorization may be written, over the phone and recorded, or a written confirmation prior to withdrawal.

* Sources of auto debits:

Some of the sources or institutions with whom you would typically set up an auto debit include: banks, businesses, non-profit organizations, and payment companies like PayPal. The institution may offer auto debit or you may request the service yourself.

* What are the Pros & Cons of auto debits?

Pros:

Both consumers and institutions are drawn to the convenience of auto debits. Consumers are attracted to auto debits because they reduce the number of bills received in the mail, there is less worry that a bill will be lost or stolen, there is no need to worry about a missed payment, and there may be a financial incentive (discount) for switching payments to an auto debit.

Companies and organizations like auto debits because they are guaranteed a timely payment and their operational costs are reduced (mailing statements, processing payments, and collections).

Cons:

Unfortunately, the cons or drawbacks of auto debits fall primarily on you, the consumer. The primary concerns regarding auto debits lie with the added risk of unforeseen fees, error, or fraud.

Because payments are automatic, you have less control as to when a payment is withdrawn and the amount that is withdrawn from your bank account. For example, if you establish an auto debit for your credit card, the amount withdrawn may be a dollar amount that you set or the minimum payment amount. Either way, your control over the amount sent each month has been restricted.

Mistakes can be very frustrating and negate the convenience associated with auto debits because you still need to keep an eye on your banking statement to ensure that the correct amount has been withdrawn. A common mistake involves incorrect withdrawal amounts. Another involves continue debit withdrawals after the bill or obligation is paid in full.

With auto debits there is also a risk of overdraft of insufficient funds fees. If your bank account has insufficient funds at the time the auto debit is withdrawn, you will likely assess an overdraft or insufficient funds fees.

When considering auto debit, you should ask if there are any fees associated with stopping or discontinuing use auto debit. There may be bank fees to correct payments or fees assessed by the company or organization to discontinue payments via auto debit.

Scammers use auto debit to gain access to your bank account. Scammers will use inducements such as a special offer, prize, or to fix a banking error. In addition, scammers can be very persuasive and insistent that time is of the essence. As a consumer, you should be wary on unsolicited phone, e-mail, or mailer requests for your checking account information. Some of the warning signs that you may be dealing with a scammer include: unsolicited contact by a telemarketer, an offer that sounds too good to be true, requesting your checking account number to “verify” that you qualify for the prize or offer, or requesting that you read the numbers (your account and routing number) at the bottom of a check.

* Consumer Protections:

The Electronic Fund Transfer Act (EFTA) was enacted in order to establish rights and responsibilities for both consumers and establishments engaging in electronic fund transfers. The EFTA provides consumers with some protections from error, loss, or theft regarding electronic fund transfers.

Consumer protections related to auto debits include: information that must be provided to the consumer, permission requirements, and how consumer complaints must be handled. When you are granting permission for funds to be withdrawn from your account, you must be given the following information: name of the company/organization, the debit amount (this may vary in the case of utility bills for example), duration of the auto debit or the number of payments, and contact information of the company/organization.

The company or organization must also have your express permission to access your bank account and withdraw funds. The express permission may be in one of the following forms: written authorization, authorization by tape-recorded phone conversation, or written confirmation prior to withdrawal.

Consumer complaints to a financial institution regarding fee errors and incorrect or fraudulent auto debits must be investigated by that institution promptly. It is important to note that if there are discrepancies or you suspect fraud, contact the company’s billing department and notify your bank immediately. There are time restrictions that limit your ability to contest errors and get your money back. Also, consider contacting your state Attorney General if you believe that you are a victim of fraud.

* Are auto debits right for you?

Auto debits have their benefits and drawbacks. That being the case, when considering whether auto debits would be right for your personal and financial situation, there are few best practices to keep in mind.

Consider limiting your auto debits to bills and transactions that have a consistent billing amount. Auto debits with variable billing amounts (ex: cell phone bill) are harder to monitor for mistakes.

Monitor auto debit withdrawals closely and frequently. If applicable, know when your last payment is due. A common problem with auto debits is that you are billed after your balance is paid off.

If you discover discrepancies, contact your bank and the company’s billing department as soon as possible. Finally, avoid unsolicited phone, e-mail, and mail requests for auto debits because these are typically associated with scams. Contact your state Attorney General if you believe that you have been a victim of fraud.

* **Account Keeping**
* Best Practices:

Good account keeping starts with protecting your accounts and personal information. Protecting your personal information is a best practice for many areas of our daily lives. There are several best practices and tips to protect your personal information when banking and account keeping.

First, you should not give out your account number, PIN number, or social security unless it is absolutely necessary. For example, if you receive a call from someone identifying themselves as calling from your bank and they are requesting personal information, ask what the issue is and tell them you will call them back. Then call back using the bank’s official contact number, not the number that the caller provided you. Calls such as these are commonly scammers who are “phishing” for your personal information in order to gain access to your bank account and steal your identity.

Do not carry your checkbook or social security card unless you know you will need it. In addition, limit the amount of pre-printed information on your check, such social security number and driver’s license number.

Everyday you probably receive numerous pieces of mail with personal identifiers on them, like your name, address, and account numbers. Protect your personal information by shredding documents that have your address and other personal information or identifiers on them.

When shopping or banking, shield the keypad when entering your PIN number at ATMs and point-of-sale registers. In addition, do not use 1234 or some other easily discoverable PIN number and don’t write your PIN number down – memorize it.

You should also avoid online banking on a public computer or on a public wireless (WiFi) account. Hackers love free WiFi, which are usually unsecured networks. Hackers have ways to capture the information entered over the unsecured network. In addition, you never know if someone is looking over your shoulder and seeing your personal banking information.

The next tip is to create a budget and stick to it. When creating your monthly or bi-weekly budget, it is a good idea to overestimate each of your monthly costs. Overestimating your monthly costs will provide you with a cushion for unexpected costs and seasonal adjustments in utility costs. In addition, cushioning your budget can lessen the likelihood of fees for insufficient funds or overdrafting on your account.

You should also check your account regularly. This means balancing your check book, including debit and online transactions. In addition, review your bank statements and compare your check book and bank statements to the balance and transactions posted on your online banking account (if applicable).

Make sure your banking institution is FDIC insured. An FDIC insured bank means that your deposits are protected or insured by the U.S. government up to $250,000 even if the bank fails. The types of accounts that are protected include: checking, savings, money markets, and CDs.

Know your banking institutions fees and policies, such as: checking fees, transactional fees, insufficient funds fees, overdraft fees, and whether the bank processes the largest checks and transactions first.

Consider overdraft protection, because it avoids the consequences of a bounced check. However, it may not avoid the fees assessed for overdrafting, which may be sizable depending on the institution. The typical overdraft fee is $35 per transaction.

Choose a banking institution that offers the services that fit your needs and lifestyle. Some of the services or convenience to take into consideration include: branch locations and hours, ATM access, daily withdrawal limits, free services (free checks or complimentary safe deposit boxes), check policies and fees, and online banking services.

* Common Mistakes:

A common mistake is “check floating.” Floating a check is essentially a gamble that your account will register your deposit(s) before the check is cashed and funds are withdrawn from your account. Writing a check when there are insufficient funds in your account is a risky and potentially costly mistake, because you could be hit with fees, harm your credit, and harm your ability to write checks in the future.

Similarly, not waiting for a deposit to clear before spending funds is different from “floating” in that a deposit has been made to your account at the time you write the check; however, your bank has not yet released the deposited funds. But, this mistake has the same effect as “floating.”

Check processing used to have a “lag time.” The lag time would be the time between writing a check and the bank processing the check and removing the funds from your account. This common mistake is related to “floating” a check in that you are gambling that there will be sufficient funds by the time the check is processed. Assuming there is a lag time exposes you to the risk of penalty fees. Prior to the Clearing for the 21st Century Act of 2004, known as “Check 21,” there was a significant lag time for processing checks because the financial system had to rely on postal services, which was subject to the effects of weather and other disasters. Check 21 drastically cut lag times because it allows banking institutions to process checks electronically rather than the physical delivery and processing of checks. Here is a common example of electronic check processing that you may see in your every day life. Let’s say you go to a grocery store and write a check. You may see the grocery clerk push your check through a scanner attached to the register. Your check has just been electronically processed and the funds from your checking account will be withdrawn relatively quickly if not immediately.

Another common mistake is to assume that checks and transactions are processed in order. Unfortunately, this is usually not the case. Banks will usually act in their own best interests not yours, which includes how they process checks. Many banking institutions cash the largest checks first. For example, over three days, you write three checks: (day 1) $40, (day 2) $125, and (day 3) $28. You had $115 in your account on day one and you expect a $500 check to be deposited into your account sometime on day two. Even though you wrote the $40 check first, and had sufficient funds to cover it, the $125 check may be cashed first resulting in insufficient funds or overdraft fees.

Post-dating checks is the practice of writing the date that the check should be cashed. The mistake with this practice is that payees are under no obligation to hold your check. Post-dating a check provides you no protection if it is cashed before the date written on the check. If you have insufficient funds on the date that the check is cashed, regardless of the date written on the check, you will be held responsible for having non-sufficient funds.

Not closing an account properly is another common mistake. Don’t assume that a zero balance or lack of activity for a significant amount of time closes the account. Fees can still accrue, leading to a negative balance and more fees. Contact your banking institution to formally close the account.

Having a joint account or co-signing on another’s account is not necessarily a mistake, but this is an area for caution. For both joint and co-signed accounts, both account holders may be held responsible for account transactions. The word of caution is this: you should not enter into a joint or co-sign an account lightly.

* **Identity Theft**
* Types of Identity Theft:

There are generally four types of identity theft and all of them can have a financial impact.

Financial identity theft is the use of personal information, ATM, debit, and credit cards to open accounts, drain bank accounts, and make purchases. For example, let’s say you go out to dinner and use your credit card to pay the bill. The waiter takes the card and walks away to process the transaction. On his way to do this he also swipes the credit card with a reader that he has in his pocket. The waiter now has your credit card number, your name, and the card’s security code in a matter of seconds. The next day the waiter/identity thief makes several online transactions, maxing out the balance.

Medical identity theft is the use of your personal info to get medical care. For example, after reviewing your medical insurance statement, you throw it away without removing personal information/identifiers. A thief takes advantage of trash bins that were put out the night before for pick-up and proceeds to go through your and your neighbor’s trash looking for personal information to use. He finds your discarded statement and uses your insurance information to see a physician, obtain medical care, and several prescriptions.

Tax identity theft is the use of your social security number to get a job or to take your tax refund. For example, let’s say you lost your wallet while on vacation. You called your bank and credit card companies, but you forgot that you were carrying your social security card with you. A year goes by and you file your federal tax return. Soon after you receive a notice from the IRS, stating that you have unreported wages. When your wallet was stolen, an identity thief sold your social security number to someone so that they could use it to gain employment.

Child identity theft is the use of a child’s social security number and other info to obtain benefits and open accounts. For example, you start receiving calls from collection agencies for your 10 year old. You discover that there was a break in at your child’s school and student records were stolen. The identity thief used school records of several children to open credit card accounts in their names.

* What do you do if you are a victim?

If you think you may have been a victim of identity theft, you should take action as soon as possible. First, contact one of the credit reporting agencies (Equifax, Experian, TransUnion) and request that a fraud alert be placed on your credit report.

Second, contact the business or financial institution where suspected fraudulent transaction(s) took place and let them know that you have been a victim of identity theft.

Third, order a free copy of your credit report and continue monitoring your credit periodically. You are entitled to one free credit report per year. [www.annualcreditreport.com](http://www.annualcreditreport.com)

Fourth, if there are fraudulent transaction(s), create an identity theft report (affidavit) with the FTC. <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> The FTC’s site for identity theft provides links to create the affidavit, contact information for credit reporting agencies, and very useful checklists.

Fifth, file a police report.

Finally, keep a detailed record of all phone calls and correspondence.

* Protecting Your Personal Information:

The goal of presenting this information is to help you avoid being a victim of identity theft in the first place. So, let’s take a look at how to protect your personal information from would be thieves. Some of these same strategies were provided to you during our discussion of safe banking and account keeping. The key point to stress when it comes to protecting your identity is to be cautious when giving or using your personal identifiers and to destroy or safely store any documents that have your information.

* Update your address and contact information with your financial institution and other businesses you have transactions with. This can help to avoid correspondence from being delivered to the wrong address and being misused. Do not rely on change of address requests through the postal service as this is only temporary.
* Do not give your account number, PIN number, or Social Security number unless it is absolutely necessary. Just as you would not hand over the keys to your house to a stranger, you do not want to freely share your personal identifiers without making sure that you trust the individual or business with whom you are sharing the information.
* Don’t be afraid to ask those who are requesting personal identifiers why they need it and what the consequences are for not providing the identifiers requested. In addition, it is a good practice to ask what will be done with any documents that have your personal information after your transaction or business is concluded. In other words, are they protecting your personal information?
* Do not carry your Social Security card with you. Memorize your number and store the card in a safe place with your other important documents. Carrying your card increases the likelihood that if your wallet is lost or stolen, your identity will be stolen as well.
* Shred any documents with personal identifiers that you no longer wish to keep. Personal identifiers include your name and address.
* Make sure that any websites that you visit and interact with are secure. Such interactions include things like banking, making purchases, and other interactions where you would provide personal information. A secure website should have “https” preceding the site address and you should also see a small padlock. In addition, it is highly recommended that you avoid using websites that require your personal identifiers while on a public wireless (WiFi) account. Hackers/identity thieves tend to target public WiFi accounts to try and capture users personal information. For example, don’t do your online banking while sitting in a coffee shop that provides free WiFi.