Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

Privacy When You Pay: Credit, Debit, Cash and More [1]

Posted Jun 01 2007
Revised Jan 25 2018

1. Introduction

Once you decide to buy something, you then must determine how to pay for it. Do you hand over cash? Write a check? Use your smartphone? Pay with a credit card? Or use a debit card and have the payment automatically deducted from your bank account?

This guide seeks to inform you about your rights and outline the potential risks and benefits of different payment methods.

2. Our Recommendation: Do Not Use Debit Cards

Privacy Rights Clearinghouse recommends that consumers never use (or even carry) debit cards because of their risks and their limited consumer protections.

By reading this guide, you will understand how a lost, stolen, or otherwise compromised debit card can result in your bank account being wiped out by a thief, without using your PIN number. Even if you promptly report the loss to your bank, under federal law the bank can wait up to two weeks (or longer in certain cases) to restore the funds to your account. That could make you unable to pay your bills or withdraw cash at an ATM. If you wait too long to report the loss, you may not even be able to recover the stolen funds.

Why the concern over debit cards?

Thieves have become increasingly sophisticated in gaining access to sensitive financial information. Databases of major retailers and restaurants have been compromised by hackers. Merchant card reading devices have been surreptitiously replaced with card skimmers. Restaurant employees have secretly captured card information on hand-held card readers. If you have a debit card and your account information is compromised, funds can quickly be withdrawn from your bank account without your knowledge. Your account can be emptied, resulting in overdrafts, fees, and an inability to pay your bills.

On the other hand, if you use a credit card, you will have an opportunity to dispute a fraudulent transaction before you have to pay the bill, so you will still retain access to the funds in your bank account.

But my bank offers a debit card fraud guarantee, so I'm covered, right?

Not exactly. Many banks do offer a fraud guarantee, and your fraudulently removed funds are likely to be replaced eventually, assuming that you comply with the specific requirements of your bank's fraud guarantee program. The key word here is *eventually*. The important thing to note is that the bank is not obligated to restore the funds to your account for at least two weeks while it investigates. During this time period, you may not have your funds available in your account to pay your mortgage, rent, loans, or other bills. Many people cannot afford to be without their money for that length of time.

Don't I need a debit card to get cash from an ATM machine?

Not necessarily. You can ask your bank to replace your debit card with an ATM card. With an ATM card, a PIN is always necessary to complete a transaction. ATM cards cannot be use for online, telephone, or mail transactions. If your ATM card is lost, stolen, or compromised, it cannot be used without your PIN. A debit card can be used by a thief without knowing your PIN.

How can I tell if my card is an ATM card or a debit card?

A debit card will have a Visa or MasterCard logo on the *front* of the card. ATM cards will *not* have a Visa or MasterCard logo on the *front* of the card. Both ATM and debit cards may have the logos of ATM networks (such as Star, Co-Op, and Allpoint) on the *back* of the card.

I don't like to carry cash. How can I pay for my everyday purchases without using a debit card?

If you enjoy the convenience of paying for your everyday purchases with plastic, consider opening a no annual fee credit card account with a small line of credit for those purchases. Be sure to promptly pay off your bill in full each month to avoid any fees and finance charges. We recommend that you do not use any credit cards on which you carry a balance for this purpose, as that would increase your finance charges.

Are there places where it is particularly risky to use a debit card?

Four especially risky places to use a debit card are outdoor ATMs, gasoline pumps, online, and at restaurants.

- Outdoor ATMs (particularly those in low traffic areas) are at higher risk for card skimming devices and pinpoint cameras than ATMs located inside a bank or business.
- Gasoline pumps pose an extraordinarily high risk for skimming. Skimming devices on gas pumps can be impossible to detect because they may be located inside the pump and utilize Bluetooth technology.
- Online transactions are risky because card information may be compromised at multiple points. Malware can steal data from your computer or other device, unsecured Wi-Fi is subject to eavesdropping, and it can be difficult to assess security at the vendor's site.
- Restaurants are high risk locations because servers generally must take your card to pay your check. While the card is out of your view, they can use a portable skimmer to copy the information from your card.

As a practical matter, there really is no safe place to use a debit card. Massive data breaches [2] such as those experienced by Target, Michaels, Home Depot, TJX (Marshalls and TJ Maxx), Neiman Marcus, and numerous hotel chains have exposed the information of millions of cardholders at thousands of locations.

3. Credit Cards

When you use a credit card, a merchant, going through the card network, electronically contacts your card issuer (usually a bank) to verify your account number, expiration date, and credit availability. Once that information is verified, the card network authorizes the transaction. The merchant then is paid by the card network, and the card network collects the money from the card issuer, which bills you in your next statement. You can choose to pay the bill in full each month without interest or extend the payments over a number of months or even years while paying interest.

***Pluses*:**

1. With credit cards and charge cards, you can buy now and pay for the goods and services later. Used with discipline, no-fee credit cards are basically free, 30-day loans. This allows users to hold onto money longer while earning interest on balances before paying bills.
2. Many cards offer extras, like rewards programs—cash rebates or points that can be exchanged for airline tickets, gift certificates, or merchandise—and extended warranties on purchases, along with car-rental insurance coverage.
3. Widely accepted and easy to use, credit cards and charge cards can be especially helpful in emergencies, such as when you encounter unexpected health-care costs or expensive auto repairs.
4. Strong consumer protection is another big advantage of credit cards. *Credit cards generally offer the best legal remedies against billing errors, defective merchandise and other consumer problems* (see below).

***Minuses*:**

1. Interest charges, fees, and penalties can mount up, especially if you don't comprehend the details of how your card works. With many cards charging 24% or more interest on an unpaid balance, consumers can end up paying many more times the

price of the item they bought.
2. Identity theft often involves fraudulent credit card use. A crook may use your credit cards in a variety of ways. Unauthorized charges may be made using your account information.

What are the consumer protections available for credit card transactions?

There are *three* distinct protections available for consumer *credit card* transactions:

- The first credit card protection shields you against liability for unauthorized use of your credit card, that is, when someone steals or otherwise uses your card or card number without permission.
- The second protection involves disputes about your bill (billing errors). These disputes may include a merchant overcharging you or charging you for products you never received.
- The third protection is the right to stop payment. Stopping payment is a powerful tool that you can use when you are dissatisfied with the quality of goods or services that you paid for with a credit card.

Remember that these three consumer protections *only* apply to transactions made with a *credit card*. They do *not* apply to debit card transactions.

What do I do about unauthorized credit card charges?

The Fair Credit Billing Act (FCBA) limits your loss from unauthorized charges to $50. However, if you report the loss *before* your credit card is used, the FCBA says you are not responsible for any charges you didn't authorize. If your credit card number is stolen, but *not the card*, you are not liable for any unauthorized use.

To dispute unauthorized credit card purchases under the FCBA, write to the creditor within 60 days after the first bill containing the error was mailed to you. Use the address given for "billing inquiries," not the address for sending your payments. Send the letter certified mail, return receipt requested. Include your name, address, account number, and a description of the billing error, including the amount and date of the error.

The Consumer Financial Protection Bureau (CFPB) is responsibility for enforcing laws related to credit card transactions. Complaints about credit card companies can be made to the CFPB [3].

What are contactless credit cards?

Some credit cards now contain embedded Radio Frequency Identification (RFID) chips which enable "contactless payments." These "contactless" cards can either be waved in front of a merchant's special reader or swiped through a traditional point of sale terminal. The RFID chip has your personal credit card information embedded in it, which can then be read by the merchant's point of sale terminal. To minimize accidental reading of these cards, they are designed to be read at a distance of one to four inches from the reader. RFID chips should not be confused the chips contained in EMV cards (described in the next question).

Unfortunately, scanners that can read RFID cards are available to the general public, including persons with fraudulent intent. Scanners can be used to interrogate the RFID card and retrieve the cardholder's account information. The credit card issuers generally contend that contactless credit cards are safe, either through use of encryption and/or with the use of dynamic one-time only numbers. Regardless, we recommend that you use an RFID-blocking wallet or sleeve for your contactless credit card.

What are EMV, "chip and PIN" or "chip and signature" credit cards?

EMV (Europay, MasterCard and Visa) is a global standard for authenticating credit and debit card transactions. EMV cards are smart cards that have a chip embedded into the card. In most countries outside the U.S., a cardholder must enter a PIN to authenticate the transaction. Unlike traditional credit cards, EMV cards do not rely on a magnetic stripe on the back of the card. EMV cards are considered to provide greater security than traditional credit cards. EMV cards are the standard in Europe.

Most U.S. chip cards are "chip and signature" rather than the European "chip and PIN" cards. Chip cards will continue to have magnetic stripes on the back to accommodate merchants that do not have chip readers. The chip stores the same information as the magnetic stripe on your credit card. The chip also contains additional security components not found on the magnetic stripe. As more U.S. merchants have developed the capability to accept chip cards, credit card fraud has dropped [4] significantly.

Chip cards differ from contactless credit cards and they generally do not contain RFID chips. In order to use a chip card, you must insert or "dip" the card into a merchant's reader. You do not "swipe" the card.

Do I always need to sign for my credit card purchases?

For many years, cardholders were required to sign their name when using a credit or debit card. According to Mastercard, more than 80 percent [5] of in store transactions in North America do not require a cardholder signature at checkout. Starting in April 2018, Visa, Mastercard, American Express and Discover will no longer require signatures [6] at checkout for credit card purchases in the U.S. for merchants who have switched over to chip readers or for contactless payments.

May a merchant require a minimum purchase when I pay with a credit card?

A merchant can require a minimum purchase when you pay by credit card, as long as the minimum purchase amount is not greater than $10. Most businesses have chosen not to implement a minimum purchase requirement, but they are free to do so as long as the minimum does not exceed $10.

Can a merchant add a surcharge or "checkout fee" when I pay by credit card?

It depends upon the state where the merchant is located. A November 2012 class-action settlement with Visa and MasterCard allows "checkout fees" to cover the cost of processing the credit card transaction, except in the 10 states where these fees are prohibited by law.

California, Colorado, Connecticut, Florida, Kansas, Maine, Massachusetts, New York, Oklahoma and Texas have laws making credit card surcharges unlawful [7]. However, these laws may only apply to certain types of transactions, and do not necessarily prevent offering a discount for paying by cash.

The **California** ban on credit card surcharges applies to private businesses, but does not apply to government agencies or public utilities. It specifically allows discounts for cash payments. California Civil Code Section 1748.1(a) provides:

No retailer in any sales, service, or lease transaction with a consumer may impose a surcharge on a cardholder who elects to use a credit card in lieu of payment by cash, check, or similar means. A retailer may, however, offer discounts for the purpose of inducing payment by cash, check, or other means not involving the use of a credit card, provided that the discount is offered to all prospective buyers.

Can a merchant put a “hold” on my card for more than I spend?

A “hold" is when a merchant tells your bank to set aside a certain amount for an impending purchase. There are different rules for services like restaurants and hair salons then there are for travel businesses — hotels, car rentals, and cruise lines.

Hotels, cruise lines, and car rental companies can pre-authorize a charge. So if you’re booking a hotel, the hotel can place a hold on your card for the estimated cost of your stay, and then charge you the actual value when you check out. If it’s within a certain threshold of the estimated charge, they don’t have to go back and do a second round of authorizations.

For services with a gratuity, the initial authorization can only be for what you actually spent. If dinner was $50, then a $50 authorization appears on your account with a notice indicating that the value is subject to change. That $10 tip you added when you signed the receipt gets added later, and then you’re charged the full $60.

4. Debit Cards and ATM Cards

Debit cards (sometimes known as check cards) look—but don’t act—like credit cards. Typically, they have a Visa or MasterCard logo on the front, but (unlike a credit card) will also say “Check Card” or “Debit” somewhere on the front of the card. They work more like checks because the money is deducted directly from your bank account. You or the merchant runs the card through a scanner that enables the bank to electronically verify the funds are available and approve the transaction.

Debit cards can function either with a Personal Identification Number (PIN) (on-line transaction) or without a PIN (off-line transaction). ATM (automatic teller machine) cards only function with a PIN (on-line transaction).

- An “on-line transaction” deducts the money from your account almost immediately and for safety reasons, requires you to give a Personal Identification Number, or PIN. PIN transactions take money from your account via electronic fund transfer (EFT), networks such as Pulse, Interlink, Star, or NYCE.
- An “off-line transaction” may not transfer the funds for a few days, and you generally sign a receipt instead of using a PIN. Signature purchases generally go through the MasterCard, Visa, or Discover networks, just like a credit card.

Merchants often steer customers toward using the PIN-type card because banks get higher fees from retailers when consumers use signature cards. A merchant may also offer a discount or incentive to steer you towards a particular method of payment.

Banks often steer their customers toward no-PIN transactions (signature transactions) because they collect higher interchange fees for no-PIN transactions.

***Pluses*:**

1. Using a debit card is easier and faster than writing a check, and they are widely accepted by merchants. Some consumers like the sense of security they get by spending only what money they have in the bank, though in some cases that may be a false sense of security. (See “minuses.”)

***Minuses*:**

1. Debit cards don't carry the same legal protection as credit cards. Federal law limits your liability on a debit card to $50, but only if you notify your financial institution within two business days of discovery of the theft. If you wait longer than 60 days after your bank statement was mailed, you could lose all the money in your checking account, and even more!
2. Consumer protections for debit cards are not as strong as those for credit cards. Because funds are deducted from your account quickly, you do not have the option to stop payment in a dispute.
3. Debit and ATM card transactions are included in the broader category of *EFT or electronic funds transfers*. Use of these cards and your potential loss are governed by the Electronic Funds Transfer Act (EFT Act)
4. Another debit card danger arises from merchant “blocking.” Blocking occurs when a merchant routinely withholds an amount on a debit card until the transaction is fully processed. This typically occurs at hotels, gas stations, and those rental car companies that still accept debit cards. When you use a debit card, the blocked amount can cause your bank account to be overdrawn.
5. If you have opted in to your bank's overdraft transfer plan, you could incur a fee averaging $35 if a debit card transaction exceeds the available balance of your account. Note however that financial institutions are prohibited from charging fees for overdrafts on debit card transactions at "point of sale" terminals in stores *unless the individual opts in to pay those fees.* If you do not opt in, your bank's standard overdraft services won't apply to your everyday debit card transactions. These transactions typically will be declined when you don't have enough money in your account, but you will not be charged overdraft fees.
6. Consumers who use debit cards to the exclusion of credit cards may be missing an opportunity to establish their creditworthiness. Responsible use of credit cards—unlike debit cards—helps build good credit scores. A good credit score can reduce the rates that you pay on car loans, mortgages, and insurance premiums.

Does use of a PIN make debit or ATM cards safer to use than credit cards?

A PIN may give you some comfort as long you closely guard your PIN and are alert to potential scams. For example, thieves have been known to “rig” ATM machines so your account number and PIN are surreptitiously recorded when you insert your card. Account information and PIN numbers have also been captured when unwary consumers buy gas or use a debit card for purchases.

You should also use caution when using a debit card to make online purchases. Remember, however, that although *you* choose to use a PIN with your debit card, a thief can use a debit card in a non-PIN transaction, thereby emptying your bank account *without knowing your PIN*.

How much can I lose from debit or ATM card fraud?

If you report [8] a debit or ATM card missing *befor*e someone uses it, the EFT Act says you are not responsible for any unauthorized transactions. If someone uses your ATM or debit card before you report it lost or stolen, your liability depends on how quickly you report it:

- Your loss is limited to $50 if you notify the financial institution within two business days after learning of loss or theft of your card or code. But you could lose as much as $500 if you do not meet the two-day deadline.

- If you do not report an unauthorized transfer that appears on your statement within 60 days after the statement is mailed to you, you risk unlimited loss on transfers made after the 60-day period. That means you could lose all the money in your account plus your maximum overdraft line of credit, if any.

If someone makes unauthorized transactions with your debit card number, *but your card is not lost*, you are not liable for those transactions if you report them within 60 days of your statement being sent to you.

What happens after I report misuse my ATM or debit card?

The EFT Act requires the bank to investigate within the following timeline:

- The bank must investigate and resolve your complaint within **45 days**.
- For errors involving new accounts (opened in the last 30 days), point-of-sale transactions, and foreign transactions, the bank may take up to **90 days** to investigate the error.
- If the bank takes **longer than 10 business** days to complete its investigation, generally it must put back into your account the amount in question while it finishes the investigation. For new accounts, the bank may take up to **20 business days** to credit your account for the amount you think is in error.
- If it finds no error, the bank must explain in writing why it believes no error occurred and let you know that it has deducted any amount re-credited during the investigation. You may ask for copies of documents relied on in the investigation.

The important thing to note is that the bank is not obligated to restore the funds to your account for 10 or 20 business days while it investigates. During this time period, you may not have your funds available in your bank account to pay your mortgage, rent, loans, or other bills. Contrast this with a *credit card* dispute, in which you have access to the money in your bank account during the investigation.

What if the bank doesn't believe I've been a victim?

You can file a complaint [9] against the bank or other financial institution. Even though the EFT Act requires an investigation, some financial institutions may give your complaint a cursory look, send you a "form" letter and refuse to restore your money. If this happens, be persistent, and, if necessary, speak with an attorney about your options.

5. Gift Cards and Prepaid Cards

Gift Cards

A gift card is generally identified by a specific number or code and not with an individual name. Thus, most gift cards can be used by any person in possession of the card. If a gift card is lost or stolen, its value may be lost. Therefore, you should treat the gift card like cash. Some gift cards can be registered by the owner, providing a mechanism for reporting lost or stolen cards.

When you purchase a gift card, be sure to read the terms and conditions (which may be printed on the card or its packaging). Provide both the terms and conditions and the receipt to the gift card recipient.

Once you have spent the entire value on the gift card, you may still want to keep it in case you need to return merchandise that you have purchased with the card. Some retailers will only allow you to return merchandise when you present the original form of payment.

Federal law [10] provides important consumer protections that apply to gift cards sold on or after August 22, 2010. These rules apply to both store gift cards, which can be used only at a particular store or group of stores (such as a book store or clothing retailer, also known as "closed-loop cards") and bank-issued gift cards (such as those with a MasterCard, Visa, American Express, or Discover logo, also known as "open-loop cards"). The law provides the following protections:

Limits on expiration dates. The money on your gift card will be good for at least five years from the date the card is purchased. Any money that might be added to the card at a later date must also be good for at least five years.

Limits on fees. Gift card fees typically are subtracted from the money on the card. Under the new rules, many gift card fees are limited. Generally, fees can be charged only if you haven't used your card for at least one year and you are only charged one fee per month. These restrictions apply to fees such as dormancy or inactivity fees for not using your card, fees for using your card (sometimes called usage fees), fees for adding money to your card, and maintenance fees.

You can still be charged a fee to purchase the card and certain other fees, such as a fee to replace a lost or stolen card. Make sure you read the card disclosure carefully to know what fees your card may have.

In some states [11], consumers are protected by both the federal law and state gift card laws.

In *California*, most gift cards cannot have *any* expiration dates or service fees. In this respect, California law is more consumer friendly than the federal law. However the California law does not apply to multiple retailer gift cards such as mall gift cards or bank gift cards including Visa and MasterCard gift cards. For those types of gift cards, only the federal law would apply.

The California gift card law is complex [12] and does not apply to all gift cards. There are numerous exceptions to the California gift card law. One unusual benefit of the California law is that a gift card with a remaining balance of less than $10 is redeemable in cash for its remaining cash value.

With many retailers recently filing for bankruptcy, you should be aware of the rules governing gift cards in a bankruptcy proceeding. A gift card sold by a seller that seeks bankruptcy protection may have no value. However, the holder of the gift card may have a claim against the bankruptcy estate. Sellers that file "Chapter 11" (reorganization) bankruptcy intend to stay in business, so they typically will ask the bankruptcy court for permission to honor gift cards in an effort to maintain good customer relations. If the bankruptcy court does not allow gift cards to be honored, or if the seller files "Chapter 7" (liquidation) bankruptcy, holders of gift cards are creditors in the bankruptcy case.

If you have received a gift card that you don't need or want, don't fall victim to a gift card resale scam [13].

Prepaid Cards

Prepaid cards are similar to debit cards. However, they are not tied to your bank account. You must initially load the card with funds and you may add more as needed. Prepaid cards can be purchased at many retailers and online. You can use the cards anywhere that credit or debit cards are accepted.

Prepaid cards may have a Visa, MasterCard, or American Express logo and the word “debit” printed on the front of the card. Typically, the card’s value is recorded on a remote database, which must be accessed for payment authorization.

Some consumers use a prepaid card as a substitute for a bank account. Others use it one as in addition to a bank account. Consumers Union has rated [14] prepaid card brands depending upon how you plan to use the card.

Some prepaid cards allow you to have your paycheck automatically deposited by your employer through direct deposit. Many also allow cash withdrawals at ATM networks. Prepaid cards can be useful as an alternative to credit cards if you find it difficult to stick to a budget. However, a prepaid card will not help you build a credit history.

Unfortunately, many prepaid cards impose multiple fees [15] on consumers. Moreover, when prepaid cards are lost or stolen, consumers may not protected. Federal laws do not limit the liability of prepaid card users for fraudulent or unauthorized use. Therefore, consumers may face significant risk of loss when using a prepaid card. However, some cards may offer "zero liability" protection in the event of fraudulent activity.

New consumer protections [16] including increased disclosures for prepaid cards will become effective on April 1, 2019.

6. Checks, Money Orders, and Cash

Checks

The Uniform Commercial Code (UCC), a version of which has been adopted by most states, includes consumer protections against check fraud. Generally, the UCC holds the bank responsible for fraudulent checks as long as you, the customer, exercise “reasonable” care, such as timely reporting.

Cashier’s Checks and Money Orders

Like personal checks processed conventionally, cashier’s checks and money orders are governed by the terms of your state’s version of the UCC. If you purchase these products from a bank, post office, or other reliable source, you can be assured that they are legitimate.

Your greatest risk involves accepting a cashier’s check or money order from someone who owes you money. Many consumers have become victims of fraud [17] involving a fraudulent cashier’s check.

Cash

Like any other payment method, there are advantages and disadvantages in always paying by cash. On the one hand, you don’t have to worry about credit scores or overdraft fees. But, if your cash is lost or stolen, you do not have the protections you may have with other forms of payment.

Additionally, currency has always been a prime target for counterfeiting [18]. Just as government printing techniques have changed to make official currency harder to duplicate, counterfeiters are ever employing the latest technology. If you suspect a counterfeit bill, report it to the U.S. Secret Service [19] or to your local police.

7. Mobile Payments

Mobile payment apps allow you to use a mobile device instead of credit or debit cards. Point of sale retail purchases account for the majority of mobile payments. If all works as intended, your device is all that you need to carry out a transaction with a merchant. Typically this is accomplished by way of an app offered either by a merchant or by a payment service.

Mobile wallets offered by some payment services may allow consumers to store multiple payment options, charging either a credit card, debit card, bank account, or cell phone account. Some digital wallets can store coupons and shopper loyalty card information.

What are some of the major mobile payment apps?

As of April 2017 [20], Apple Pay and PayPal led the market for in-store mobile payments. Other popular mobile payment apps include Starbucks app, Masterpass, Android Pay, Visa payWave, and Samsung Pay. Consumerist offers a summary [21] of the major mobile payment apps that describes:

- Who owns it?
- How do I fund it?
- How does it work?
- Where can I use it?

What are some of the privacy risks and other concerns about mobile payments?

Mobile payments can expose your personal information to companies that would not be included in a traditional credit card transaction. In addition to credit card issuers and payment processors, mobile payment services may involve the mobile payment provider, the internet service provider, and any third party apps that consumers download. With mobile payments, these companies can get access to the consumer information revealed during a traditional credit card transaction and use this information in new ways.

A Federal Trade Commission staff report Paper, Plastic…or Mobile?: An FTC Workshop on Mobile Payments [22] notes three major areas of potential concern for consumers. The report encourages companies to develop clear policies on how consumers can resolve disputes arising from a fraudulent mobile payment or an unauthorized charge. It also encourages industry-wide adoption of strong measures to ensure security throughout the mobile payment process. Finally, the report notes the privacy issues arising from the consolidation of consumers' personal information in the mobile payment process. In a traditional credit card transaction, a merchant will have sensitive financial information about consumers, but will generally not also have their contact information and a record of their location. Mobile payment providers also potentially have access to a much larger cache of personal information stored on the consumer's mobile device.

Before you consider making a payment with your mobile device, be aware of any fees that may be associated with using the service. Also, you need to be aware that your legal protections may vary, depending upon the underlying payment mechanism tied to your device.

What laws protect payments from a mobile device?

A typical mobile payment transaction may involve a merchant, a wireless carrier, a payment service, and a bank. Unfortunately, the law often does not develop as rapidly as technology. As a result, your legal protections when paying with a mobile device will depend upon the underlying payment mechanism connected to the device. This might be a credit card, debit card, or the charges might appear directly on your cell phone bill.

How can I make my mobile payments more secure?

If you have enabled mobile payments on your device, make sure to treat the device the same as you would your wallet or purse. People are much more likely to leave a cell phone unattended then they would a traditional wallet. Make sure that you keep your device locked with a password.

It's also a good idea to double password protect any payment mechanism. That is, have one password for your mobile device and a different password for the payment mechanism itself. Also, make sure that any downloaded payment apps come from reliable and trustworthy sources. Finally, use any security software that may be available for your particular device.

8. Peer-to-Peer (P2P) Payments

Peer-to-Peer or Person-to-Person or (P2P) payments enable consumers to send, receive, or request a payment to or from

another person. They are most frequently used for small payments, such as sharing the cost of a restaurant bill, sending a cash gift, or paying a babysitter. Some people predict that P2P will replace [23] cash and check payments by the end of the decade.

P2P services are generally intended for the transfer of money from one person to another person that you already know. Most P2P services cannot be used for commercial purposes, although some can be used to make payments to merchants who have chosen to accept P2P payments.

Opening a P2P account generally requires you to establish a payment source. This could be a bank or credit union deposit (checking or savings) account, a credit card, or a prepaid card. Funds used to pay people will be taken out of the source account. Some P2P services will hold your funds within your P2P account itself (stored value or digital wallet), rather than accessing your money from an external source each time that you make a payment.

When you want to send money to someone, you'll need to provide the P2P service with the recipient's email address or mobile phone number. To obtain money, recipients generally need to provide their bank account information to the sender's P2P provider.

P2P services are often accessed through a smartphone app, but many can also be used through your computer.

Venmo, PayPal, Square Cash, Google Wallet, and Facebook all offer P2P services. Zelle is a unified P2P service sponsored by more than 30 U.S. banks and credit unions.

There are a number of things to consider when using a P2P app:

- Understand the P2P service's privacy policy. It should explain how your personal information (and that of your recipients) is used and shared. Find out if information about your transactions will be shared with other users, such as your social media friends. Set any available privacy settings to the most restrictive settings to avoid oversharing. Remember that privacy policies and settings may change, so periodically re-check them.
- Avoid making payments to people you don't know, particularly for selling or buying things from strangers. A buyer/scammer can often cancel a P2P transfer [24] after receiving the goods but before the money is taken out of their account.
- Learn how the P2P service handles disputes and complaints. For example, what happens if the service pays the wrong person or the wrong amount? If the funds are withdrawn from a bank or credit card account, you will have certain rights under federal law. But if the funds are held in a stored value account with the payment service, you may not have any rights beyond those set forth in the service's terms and conditions.
- Consider the benefits of using a bank sponsored P2P service, rather than a non-bank service. Your funds will be protected by federal deposit insurance while they are in a bank or a federal credit union. Funds sitting in non-bank P2P service may not have this protection.
- Be aware of any possible costs or fees, such as a fee to send or receive payments. Generally, you can make P2P payments from a linked bank account or from the P2P account for free. Some providers charge fees to process payments from a credit or debit card.
- Make sure that the P2P service is set up to send you an email or text message any time there's a transaction on your account.
- If using the P2P service for business purposes, rather than personal payments, make certain that the service allows commercial payments.
- Recognize that transferred funds may not be immediately available. This could depend upon the particular P2P service and the receiving financial institution.

9. Resources

U.S. Government Publications

- FTC Facts for Consumers: *Credit Cards, ATM Cards, Debit Cards, What to Do If They're Lost or Stolen* [8]
- FTC Facts for Consumers: *Disputing Credit Card Charges* [25]

Source URL (modified on January 25, 2018): https://www.privacyrights.org/consumer-guides/privacy-when-you-pay-credit-debit-cash-and-more

Links

[1] https://www.privacyrights.org/consumer-guides/privacy-when-you-pay-credit-debit-cash-and-more
[2] http://www.privacyrights.org/data-breaches
[3] https://help.consumerfinance.gov/app/ask_cc_complaint#active_tab=vcomplaint

[4] https://www.usatoday.com/story/money/personalfinance/budget-and-spending/2017/12/29/heres-proof-that-the-emv-chip-in-your-credit-card-is-working/108994136/
[5] https://newsroom.mastercard.com/2017/10/19/no-more-signing-on-the-dotted-line/
[6] https://www.theverge.com/2018/1/12/16884814/visa-chip-emv-signatures-north-america-credit-card-april-2018
[7] http://www.electronicpaymentscoalition.org/settlement-consumers/
[8] https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards
[9] https://forms.federalreserveconsumerhelp.gov/secure/complaint/formComplaint
[10] http://www.consumerfinance.gov/about-us/blog/giving-or-receiving-gift-cards-know-the-terms-and-avoid-surprises/
[11] http://www.ncsl.org/research/financial-services-and-commerce/gift-cards-and-certificates-statutes-and-legis.aspx
[12] http://www.dca.ca.gov/publications/legal_guides/s-11.shtml
[13] http://www.fraud.org/giftcard_resale_alert
[14] http://www.consumerreports.org/prepaid-cards/prepaid-cards-are-getting-better/
[15] http://www.consumer-action.org/modules/articles/a_consumers_guide_to_choosing_a_prepaid_card
[16] https://www.consumerfinance.gov/prepaid-rule/
[17] https://www.occ.gov/news-issuances/consumer-advisories/2007/consumer-advisory-2007-1.html
[18] https://www.treasury.gov/about/organizational-structure/offices/Treasurer-US/Pages/if-you-suspect.aspx
[19] http://www.secretservice.gov/contact/field-offices/
[20] https://www.statista.com/statistics/712881/instore-mobile-wallet-usage-usa/
[21] http://consumerist.com/2016/02/02/tap-or-scan-here-to-pay-know-your-mobile-payment-apps/
[22] http://ftc.gov/os/2013/03/130306mobilereport.pdf
[23] http://www.thepaymentsreview.com/a-look-at-p2p-payments
[24] https://www.bbb.org/council/news-events/bbb-scam-alerts/2016/scammers-use-venmo-to-fool-sellers
[25] https://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges