This article is about all types of credit card fraud. For organised trade and laundering of credit card information, see Carding (fraud).

Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card.[1] The purpose may be to obtain goods or services or to make payment to another account, which is controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help financial institutions process card payments securely and reduce card fraud.[2]

Credit card fraud can be authorised, where the genuine customer themselves processes payment to another account which is controlled by a criminal, or unauthorised, where the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party. In 2018, unauthorised financial fraud losses across payment cards and remote banking totalled £844.8 million in the United Kingdom. Whereas banks and card companies prevented £1.66 billion in unauthorised fraud in 2018. That is the equivalent to £2 in every £3 of attempted fraud being stopped.[3]

Credit card fraud can occur when unauthorized users gain access to an individual's credit card information in order to make purchases, other transactions, or open new accounts. A few examples of credit card fraud include account takeover fraud, new account fraud, cloned cards, and cards-not-present schemes. This unauthorized access occurs through phishing, skimming, and information sharing by a user, oftentimes unknowingly. However, this type of fraud can be detected through means of artificial intelligence and machine learning as well as prevented by issuers, institutions, and individual cardholders. According to a 2021 annual report, about 50% of all Americans have experienced a fraudulent charge on their credit or debit cards, and more than one in three credit or debit card holders have experienced fraud multiple times. This amounts to 127 million people in the US that have been victims of credit card theft at least once.

Regulators, card providers and banks take considerable time and effort to collaborate with investigators worldwide with the goal of ensuring fraudsters are not successful. Cardholders' money is usually protected from scammers with regulations that make the card provider and bank accountable. The technology and security measures behind credit cards are continuously advancing, adding barriers for fraudsters attempting to steal money.[4]

Means of payment card fraud[edit]

There are two kinds of card fraud: card-present fraud (not so common nowadays) and card-not-present fraud (more common). The compromise can occur in a number of ways and can usually occur without the knowledge of the cardholder. The internet has made database security lapses particularly costly, in some cases, millions of accounts have been compromised.[5]

Stolen cards can be reported quickly by cardholders, but a compromised account's details may be held by a fraudster for months before any theft, making it difficult to identify the source of the compromise. The cardholder may not discover fraudulent use until receiving a statement. Cardholders can mitigate this fraud risk by checking their account frequently to ensure there are not any suspicious or unknown transactions.[6]

When a credit card is lost or stolen, it may be used for illegal purchases until the holder notifies the issuing bank and the bank puts a block on the account. Most banks have free 24-hour telephone numbers to encourage prompt reporting. Still, it is possible for a thief to make unauthorized purchases on a card before the card is cancelled.

Prevention of payment card fraud[edit]

Card information is stored in a number of formats. Card numbers – formally the Primary Account Number (PAN) – are often embossed or imprinted on the card, and a magnetic stripe on the back contains the data in a machine-readable format. Fields can vary, but the most common include the Name of the cardholder; Card number; Expiration date; and Verification CVV code.

In Europe and Canada, most cards are equipped with an EMV chip which requires a 4 to 6 digit PIN to be entered into the merchant's terminal before payment will be authorized. However, a PIN is not required for online transactions. In some European countries, buyers using a card without a chip may be asked for photo ID at the point of sale.

In some countries, a credit card holder can make a contactless payment for goods or services by tapping their card against a RFID or NFC reader without the need for a PIN or signature if the cost falls under a pre-determined limit. However, a stolen credit or debit card could be used for a number of smaller transactions prior to the fraudulent activity being flagged.

Card issuers maintain several countermeasures, including software that can estimate the probability of fraud. For example, a large transaction occurring a great distance from the cardholder's home might seem suspicious. The merchant may be instructed to call the card issuer for verification or to decline the transaction, or even to hold the card and refuse to return it to the customer.[7]

Detecting credit card fraud using technology[edit]

Artificial and Computational intelligence[edit]

Given the immense difficulty of detecting credit card fraud, artificial and computational intelligence was developed in order to make machines attempt tasks in which humans are already doing well. Computation intelligence is simply a subset of AI enabling intelligence in a changing environment. Due to advances in both artificial and computational intelligence, the most commonly used and suggested ways to detect credit card fraud are rule induction techniques, decision trees, neural networks, Support Vector Machines, logistic regression, and meta heuristics. There are many different approaches that may be used to detect credit card fraud. For example, some "suggest a framework which can be applied real time where first an outlier analysis is made separately for each customer using self-organizing maps and then a predictive algorithm is utilized to classify the abnormal looking transactions." Some problems that arise when detecting credit card fraud through computational intelligence is the idea of misclassifications such as false negatives/positives, as well as detecting fraud on a credit card having a larger available limit is much more prominent than detecting a fraud with a smaller available limit. One algorithm that helps detect these sorts of issues is determined as the MBO Algorithm. This is a search technique that brings upon improvement by its "neighbor solutions". Another algorithm that assists with these issues is the GASS algorithm. In GASS, it is a hybrid of genetic algorithms and a scatter search.[8]

Machine learning[edit]

Touching a little more on the difficulties of credit card fraud detection, even with more advances in learning and technology every day, companies refuse to share their algorithms and techniques to outsiders. Additionally, fraud transactions are only about 0.01–0.05% of daily transactions, making it even more difficult to spot. Machine learning is similar to artificial intelligence where it is a sub field of AI where statistics is a subdivision of mathematics. With regards to machine learning, the goal is to find a model that yields that highest level without overfitting at the same time. Overfitting means that the computer system memorized the data and if a new transaction differs in the training set in any way, it will most likely be misclassified, leading to an irritated cardholder or a victim of fraud that was not detected. The most popular programming used in machine learning are Python, R, and MatLab. At the same time, SAS is becoming an increasing competitor as well. Through these programs, the easiest method used in this industry is the Support Vector Machine. R has a package with the SVM function already programmed into it. When Support Vector Machines are employed, it is an efficient way to extract data. SVM is considered active research and successfully solves classification issues as well. Playing a major role in machine learning, it has "excellent generalization performance in a wide range of learning problems, such as handwritten digit recognition, classification of web pages and face detection." SVM is also a successful method because it lowers the possibility of overfitting and dimensionality.[9]

Types of payment card fraud[edit]

Application fraud[edit]

Application fraud takes place when a person uses stolen or fake documents to open an account in another person's name. Criminals may steal or fake documents such as utility bills and bank statements to build up a personal profile. When an account is opened using fake or stolen documents, the fraudster could then withdraw cash or obtain credit in the victim's name.[10]

Application fraud can also occur using a synthetic identity which is similar to the fake documents mentioned above. A synthetic identity is personal information gathered from many different identities to create one fake identity.[11] Once the identity and the account is established, the fraudster has a few different options to take advantage of the bank. They can maximize their credit card spending by spending as much money as possible on their new credit card. Many fraudsters will use the new credit card to purchase items that have a high resale value so they can turn it into cash.

Account takeover[edit]

An account takeover refers to the act by which fraudsters will attempt to assume control of a customer's account (i.e. credit cards, email, banks, SIM card and more). Control at the account level offers high returns for fraudsters. According to Forrester, risk-based authentication (RBA) plays a key role in risk mitigation.[12]

A fraudster uses parts of the victim's identity such as an email address to gain access to financial accounts. This individual then intercepts communication about the account to keep the victim blind to any threats. Victims are often the first to detect account takeover when they discover charges on monthly statements they did not authorize or multiple questionable withdrawals.[13] There has been an increase in the number of account takeovers since the adoption of EMV technology, which makes it more difficult for fraudsters to clone physical credit cards.[14]

Among some of the most common methods by which a fraudster will commit an account, takeover includes proxy-based "checker" one-click apps, brute-force botnet attacks, phishing,[15] and malware. Other methods include dumpster diving to find personal information in discarded mail, and outright buying lists of 'Fullz', a slang term for full packages of identifying information sold on the black market.[16]

Once logged in, fraudsters have access to the account and can make purchases and withdraw money from bank accounts.[17] They have access to any information that is tied to the account, they can steal credit card numbers along with social security numbers. They can change the passwords to prevent the victim from accessing their account. Cybercriminals have the opportunity to open other accounts, utilize rewards and benefits from the account, and sell this information to other hackers.

Social engineering fraud[edit]

Social engineering fraud can occur when a criminal poses as someone else which results in a voluntary transfer of money or information to the fraudster. Fraudsters are turning to more sophisticated methods of scamming people and businesses out of money. A common tactic is sending spoof emails impersonating a senior member of staff and trying to deceive employees into transferring money to a fraudulent bank account.[18]

Fraudsters may use a variety of techniques in order to solicit personal information by pretending to be a bank or payment processor. Telephone phishing is the most common social engineering technique to gain the trust of the victim.

Businesses can protect themselves with a dual authorisation process for the transfer of funds that requires authorisation from at least two persons, and a call-back procedure to a previously established contact number, rather than any contact information included with the payment request. The bank must refund any unauthorised payment; however, they can refuse a refund if they can prove the customer authorised the transaction, or it can prove the customer is at fault because they acted deliberately, or failed to protect details that allowed the transaction.[19]

Skimming[edit]

"Skimmer (device)" redirects here. For other uses, see Skimmer (disambiguation).

Green plastic unit on an ATM slot, intended to stop thieves from installing a skimmer device on the machine

Skimming is the theft of personal information which has been used in an otherwise normal transaction. The thief can procure a victim's card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' card numbers. Common scenarios for skimming are taxis, restaurants or bars where the skimmer has possession of the victim's payment card out of their immediate view.[20] The thief may also use a small keypad to unobtrusively transcribe the three or four-digit card security code, which is not present on the magnetic strip.

Call centers are another area where skimming can easily occur.[21] Skimming can also occur at merchants when a third-party card-reading device is installed either outside a card-swiping terminal. This device allows a thief to capture a customer's card information, including their PIN, with each card swipe.[22]

Skimming is difficult for the typical cardholder to detect, but given a large enough sample, it is fairly easy for the card issuer to detect. The issuer collects a list of all the cardholders who have complained about fraudulent transactions, and then uses data mining to discover relationships among them and the merchants they use. Sophisticated algorithms can also search for patterns of fraud. Merchants must ensure the physical security of their terminals, and penalties for merchants can be severe if they are compromised, ranging from large fines by the issuer to complete exclusion from the system, which can be a death blow to businesses such as restaurants where credit card transactions are the norm.

Instances of skimming have been reported where the perpetrator has put over the card slot of an automated teller machine, a device that reads the magnetic strip as the user unknowingly passes their card through it.[23] These devices are often used in conjunction with a miniature camera to read the user's personal identification number at the same time.[24] This method is being used in many parts of the world, including South America, Argentina,[25] and Europe.[26]

Unexpected repeat billing[edit]

Online bill paying or internet purchases utilizing a bank account are a source for repeat billing known as "recurring bank charges". These are standing orders or banker's orders from a customer to honour and pay a certain amount every month to the payee. With E-commerce, especially in the United States, a vendor or payee can receive payment by direct debit through the ACH Network. While many payments or purchases are valid, and the customer has intentions to pay the bill monthly, some are known as *Rogue Automatic Payments*.[27]

Another type of credit card fraud targets utility customers. Customers receive unsolicited in-person, telephone, or electronic communication from individuals claiming to be representatives of utility companies. The scammers alert customers that their utilities will be disconnected unless an immediate payment is made, usually involving the use of a reloadable debit card to receive payment. Sometimes the scammers use authentic-looking phone numbers and graphics to deceive victims.

Phishing[edit]

Phishing is one of the most common methods used to steal personal data. It is a type of cyber attack in which the attacker acts as a credible person, institution, or entity and attempts to lure the victim into accepting a message or taking action with the specific request. Often, the target of the attack will receive an email or text message about something they would possibly want or need with the hope of tricking them into opening or downloading the message. During the COVID-19 pandemic, phishing has been on the rise as our world turned even more virtual. To give perspective, "researchers noted a substantial spike of 667% in COVID-19 phishing attacks in the first months of the pandemic."[28]. Also, given the significance of health care systems over these recent years health care companies have been the main targets of phishing attacks. These companies have tons of personal data stored that can be extremely valuable to the attacker.

Information sharing[edit]

Information sharing is the transfer or exchange of data between individuals, companies, organizations, and technologies. Advances in technology, the internet, and networks have accelerated the growth of information sharing. Information is spread and shared in the matter of seconds, and is being accumulated and digested at speeds faster than ever before. People are often not aware of how much sensitive and personal information they share every day. For example, when purchasing goods online, the buyer's name, email address, home address, and credit card information are stored and shared with third parties to track them and their future purchases. Organizations work hard to keep individuals' personal information secure in their databases, but sometimes hackers are able to compromise its security and gain access to an immense amount of data. One of the largest data breaches occurred at the discount retailer Target. In this breach about 40 million shopper were affected. In this specific case, the hackers targeted their point-of-sale system – meaning "they either slipped malware into the terminals where customers swipe their credit cards, or they collected customer data while it was on route from Target to its credit card processors."[29] In just one single purchase at the register, masses of personal data is collected which when stolen has major ramifications. The financial infrastructure and payment system will continue to be a work-in-progress as it constantly is at battle with security hackers.

Regulation and governance[edit]

United States[edit]

While not federally mandated in the United States PCI DSS is mandated by the Payment Card Industry Security Standard Council, which is composed of major credit card brands and maintains this as an industry standard. Some states have incorporated the standard into their laws.

Proposed toughening of federal law[edit]

The US Department of Justice announced in September 2014 that it will seek to impose a tougher law to combat overseas credit card trafficking. Authorities say the current statute is too weak because it allows people in other countries to avoid prosecution if they stay outside the United States when buying and selling the data and do not pass their illicit business through the U.S. The Department of Justice asks US Congress to amend the current law that would make it illegal for an international criminal to possess, buy or sell a stolen credit card issued by a U.S. bank independent of geographic location.[30]

Cardholder liability[edit]

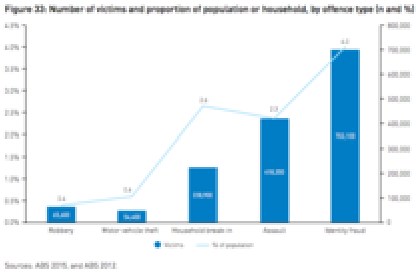
In the US, federal law limits the liability of cardholders to $50 in the event of theft of the actual credit card, regardless of the amount charged on the card, if reported within 60 days of receiving the statement.[31] In practice, many issuers will waive this small payment and simply remove the fraudulent charges from the customer's account if the customer signs an affidavit confirming that the charges are indeed fraudulent. If the physical card is not lost or stolen, but rather just the credit card account number itself is stolen, then federal law guarantees cardholders have zero liability to the credit card issuer.[32]

United Kingdom[edit]

In the UK, credit cards are regulated by the Consumer Credit Act 1974 (amended 2006). This provides a number of protections and requirements. Any misuse of the card, unless deliberately criminal on the part of the cardholder, must be refunded by the merchant or card issuer.

The regulation of banks in the United Kingdom is undertaken by the: Bank of England (BoE); Prudential Regulation Authority (PRA) a division of the BoE; and the Financial Conduct Authority (FCA) who manages the day to day oversight. There is no specific legislation or regulation that governs the credit card industry. However, the Association for Payment Clearing Services (APACS) is the institution that all settlement members are a part of. The organisation works under the Banking Consolidation Directive to provide a means by which transactions can be monitored and regulated.[33] UK Finance is the association for the UK banking and financial services sector, representing more than 250 firms providing credit, banking and payment-related services.

Australia[edit]



A graph showing the number of victims and proportion of the population or household affected by different offences

In Australia, credit card fraud is considered a form of *identity crime*. The Australian Transaction Reports and Analysis Centre has established standard definitions in relation to identity crime for use by law enforcement across Australia:

- The term **identity** encompasses the identity of natural persons (living or deceased) and the identity of bodies corporate
- **Identity fabrication** describes the creation of a fictitious identity
- **Identity manipulation** describes the alteration of one's own identity
- **Identity theft** describes the theft or assumption of a pre-existing identity (or significant part thereof), with or without consent and whether, in the case of an individual, the person is living or deceased
- **Identity crime** is a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of a crime(s).[34]

Hong Kong[edit]

Given increasing number of unauthorised payment card transactions involving frauds and scams, the Hong Kong Monetary Authority issued two Circulars on 25 April 2023. [35]

Losses[edit]

Estimates created by the Attorney-General's Department show that identity crime costs Australia upwards of $1.6 billion each year, with the majority of about $900 million being lost by individuals through credit card fraud, identity theft and scams.[34] In 2015, the Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism, Michael Keenan, released the report Identity Crime and Misuse in Australia 2013–14. This report estimated that the total direct and indirect cost of identity crime was closer to $2 billion, which includes the direct and indirect losses experienced by government agencies and individuals, and the cost of identity crimes recorded by police.[36]

Cardholder liability[edit]

The victim of credit card fraud in Australia, still in possession of the card, is not responsible for anything bought on it without their permission. However, this is subject to the terms and conditions of the account. If the card has been reported physically stolen or lost the cardholder is usually not responsible for any transactions not made by them, unless it can be shown that the cardholder acted dishonestly or without reasonable care.[34]

Vendors vs merchants[edit]

To prevent vendors from being "charged back" for fraud transactions, merchants can sign up for services offered by Visa and MasterCard called Verified by Visa and MasterCard SecureCode, under the umbrella term 3-D Secure. This requires consumers to add additional information to confirm a transaction.[citation needed]

Often enough online merchants do not take adequate measures to protect their websites from fraud attacks, for example by being blind to sequencing. In contrast to more automated product transactions, a clerk overseeing "card present" authorization requests must approve the customer's removal of the goods from the premises in real time.[citation needed]

If the merchant loses the payment, the fees for processing the payment, any currency conversion commissions, and the amount of the chargeback penalty. For obvious reasons, many merchants take steps to avoid chargebacks – such as not accepting suspicious transactions. This may spawn collateral damage, where the merchant additionally loses legitimate sales by incorrectly blocking legitimate transactions. Mail Order/Telephone Order (MOTO) merchants are implementing agent-assisted automation which allows the call center agent to collect the credit card number and other personally identifiable information without ever seeing or hearing it. This greatly reduces the probability of chargebacks and increases the likelihood that fraudulent chargebacks will be overturned.[37]

Famous credit fraud attacks[edit]

Between July 2005 and mid-January 2007, a breach of systems at TJX Companies exposed data from more than 45.6 million credit cards. Albert Gonzalez is accused of being the ringleader of the group responsible for the thefts.[38] In August 2009 Gonzalez was also indicted for the biggest known credit card theft to date – information from more than 130 million credit and debit cards was stolen at Heartland Payment Systems, retailers 7-Eleven and Hannaford Brothers, and two unidentified companies.[39]

In 2012, about 40 million sets of payment card information were compromised by a hack of Adobe Systems.[40] The information compromised included customer names, encrypted payment card numbers, expiration dates, and information relating to orders, Chief Security Officer Brad Arkin said.[41]

In July 2013, press reports indicated four Russians and a Ukrainian were indicted in the U.S. state of New Jersey for what was called "the largest hacking and data breach scheme ever prosecuted in the United States."[42] Albert Gonzalez was also cited as a co-conspirator of the attack, which saw at least 160 million credit card losses and excess of $300 million in losses. The attack affected both American and European companies including Citigroup, Nasdaq OMX Group, PNC Financial Services Group, Visa licensee Visa Jordan, Carrefour, JCPenney and JetBlue Airways.[43]

Between 27 November 2013 and 15 December 2013, a breach of systems at Target Corporation exposed data from about 40 million credit cards. The information stolen included names, account numbers, expiry dates, and card security codes.[44]

From 16 July to 30 October 2013, a hacking attack compromised about a million sets of payment card data stored on computers at Neiman-Marcus.[40][45] A malware system, designed to hook into cash registers and monitor the credit card authorisation process (RAM-scraping malware), infiltrated Target's systems and exposed information from as many as 110 million customers.[46]

On 8 September 2014, The Home Depot confirmed that their payment systems were compromised. They later released a statement saying that the hackers obtained a total of 56 million credit card numbers as a result of the breach.[47]

On 15 May 2016, in a coordinated attack, a group of around 100 individuals used the data of 1600 South African credit cards to steal US$12.7 million from 1400 convenience stores in Tokyo within three hours. By acting on a Sunday and in another country than the bank which issued the cards, they are believed to have won enough time to leave Japan before the heist was discovered.[48]

Countermeasures to combat card payment fraud[edit]

Countermeasures to combat credit card fraud include the following.

By Merchants[edit]

- PAN truncation – not displaying the full **p**rimary **a**ccount **n**umber on receipts
- Tokenization (data security) – using a reference (token) to the card number rather than the real card number
- Requesting additional information, such as a PIN, ZIP code, or Card Security Code
- Performing geolocation validation, such as IP address
- Use of Reliance Authentication, indirectly via PayPal, or directly via iSignthis or miiCard.

By Card issuers[edit]

- Fraud detection and prevention software[49][50][51][52] that analyzes patterns of normal and unusual behavior as well as individual transactions in order to flag likely fraud. Profiles include such information as IP address.[53] Technologies have existed since the early 1990s to detect potential fraud. One early market entrant was Falcon;[50] other leading software solutions for card fraud include Actimize, SAS, BAE Systems Detica, and IBM.
- Fraud detection and response business processes such as:
- Contacting the cardholder to request verification
- Placing preventative controls/holds on accounts that may have been victimized
- Blocking card until transactions are verified by the cardholder
- Investigating fraudulent activity
- Strong Authentication measures such as:
- Multi-factor Authentication, verifying that the account is being accessed by the cardholder through requirement of additional information such as account number, PIN, ZIP, challenge questions. There are five main factors to multi-factor authentication and they include:[54]

1. Knowledge - things a user knows such as passwords or answers to secret questions.
2. Possession - an object the user should have in their possession such as the actual credit card.
3. Inherence - a biological trait of the user such as finger-print or facial recognition.
4. Location - where the user is at the time of the authentication - verify the user was the one to use the card.
5. Time - when the authentication is taking place - is it a strange hour or multiple times?

- Multi possession-factor authentication, verifying that the account is being accessed by the cardholder through requirement of additional personal devices such as smart watch, smart phone challenge–response authentication[55]
- Out-of-band Authentication,[56] verifying that the transaction is being done by the cardholder through a "known" or "trusted" communication channel such as text message, phone call, or security token device
- Industry collaboration and information sharing about known fraudsters and emerging threat vectors[57][58]

- Automated Data Controls:

6. The use of automated data controls which are used to recognize when unusual activity or spending occur with a credit card. These controls can be used in real time to react "...to anything suspicious they come upon, so the flow of fraudulent activity is stopped as soon as possible..." (Johnston).[59] The three main ways automated data controls protect information includes:
7. Reconciliation and verification to ensure that the controls are working properly.
8. Continuous monitoring and alerting which alerts the cardholder/bank when unusual activity is taking place.
9. Reporting which ensures organizations have proper controls in place to prevent fraudulent activity

By Banks and Financial Institutions[edit]

- Internal self-banking area for the customer to carry out the transactions regardless of the weather conditions. The access door:
- Identifies every cardholder that gains access to the designated area
- Increases protection for customers during self-service procedures
- Protects the ATMs and banking assets against unauthorized usage
- The protected area can also be monitored by the bank's CCTV system
- Cards use CHIP identification (ex PASSCHIP [60]) to decrease the possibility of card skimming

By Governmental and Regulatory Bodies[edit]

- Enacting consumer protection laws related to card fraud
- Performing regular examinations and risk assessments of credit card issuers[61]
- Publishing standards, guidance, and guidelines for protecting cardholder information and monitoring for fraudulent activity[62]
- Regulation, such as that introduced in the SEPA and EU28 by the European Central Bank's 'SecuRe Pay'[63] requirements and the Payment Services Directive 2[64] legislation.

By Cardholders[edit]

- Reporting lost or stolen cards
- Reviewing charges regularly and reporting unauthorized transactions immediately
- Keeping a credit card within the cardholder's view at all times, such as in restaurants and taxis
- Installing virus protection software on personal computers
- Using caution when using credit cards for online purchases, especially on non-trusted websites, make sure site is reputable
- Keeping a record of account numbers, their expiration dates, and the phone number and address of each company in a secure place.[65]
- Not sending credit card information by unencrypted email
- Not keeping written PIN numbers with the credit card.
- Not giving out credit card numbers and other information online
- Sign up for transaction alerts when card is used[66]
- Be aware of phishing schemes

Disparities and Ethical Dilemmas in Credit Card Fraud[edit]

Generation Differences

10. Millennials are the biggest victims of all fraud, including credit and debit card fraud, digital wallet, digital payment, banking and tax fraud. Followed by them are the GenXers and then the GenZers.
11. Millennials spend the most time trying to recover money lost due to fraudulent charges, disputing fraudulent charges, and checking accounts for fraudulent or unusual activity out of any of the generational groups.[67]
12. GenZers experienced fraud most often through digital payment apps such as PayPal, Venmo and Square. The other generations experienced most of their issues through credit card fraud.
13. Baby Boomers were found to have the lowest instances of fraudulent charges, and also spent the least amount of time trying to recover money due to fraudulent charges or to dispute these charges.

Racial Differences

14. "The Federal Trade Commission ("FTC") and the Consumer Financial Protection Bureau ("CFPB") produced reports on the connection between minority populations and consumer issues. Each report came to the same conclusion: unfair and deceptive practices have unique and disproportionate impacts on communities of color. These findings suggest that more needs to be done to protect these communities from fraud."[68] On top of this, hackers specifically target communities of color for reasons such as their need for additional income or credit, or their tendency to use certain types of financial products.
15. Additional report findings: [68]
16. While Black and Latino consumers are more likely to experience fraud, Latino communities predominantly underreport compared with Black and White communities.
17. Latino and Black consumers report different rates of fraud concerning distinct categories of problem. The FTC found that their complaint database showed Black, and to a lesser extent Latino, communities experience higher rates of problems with credit bureaus and debt collections than White communities.
18. White and Latino communities experience higher rates of impersonator scams than Black communities. Also, according to FTC payment method data, Black and Latino communities use credit cards, with their accompanying legal protections, at a substantially lower rate than in White communities.