

Support for Enhanced Consumer Financial Protection for Victims of Prepaid / Gift Card Fraud Under EFTA

With increasingly changing tactics, criminals misuse all manners of modern-day communication and financial systems to perpetrate their fraudulent schemes on consumers daily. Massive data leaks, system breaches, and privacy glitches across industry sector lines provide an enormous amount of information about American consumers to those with nefarious intent. We are told we cannot trust our caller IDs and email—the most basic of public mass communication methods—due to “spoofing” and “phishing” because these are now favorite tools for fraudsters and scammers. Our voices can even be captured and recorded when we answer a telephone call, which can then be used to deceive our families and friends into believing we need help. Our technology has created an environment ripe for fraud and theft, and everyday normal people are the targets.

Prepaid/ gift card scams are rampant and constantly evolving with greater sophistication. Despite ongoing awareness campaigns from a wide variety of sources, this kind of information does not reach people who are going about their everyday lives: working, running errands, deciding what to cook for dinner, taking the kids to and from practice, caring for an ailing parent, or making their dollars stretch until next payday. To borrow a colloquial phrase from social media, *IYKYK*: people are, unfortunately, informed about scams when they or someone they know are scammed. By then, the financial damage is done and (most often than not) irreversible.

Financial consumer protection laws are extremely complex and difficult for ordinary people to understand and try to work out on their own. After a scam, it takes an incredible amount of time to figure out “next steps” or even where to go for help if you are not a detective, lawyer, or banker—or have enough money to just accept the loss. That is exactly when most people come to realize there is an immense amount of information on the internet about how to avoid scams, but very few solid resources on what to do after a scam. Several websites claim, “*If you are the victim of a scam, you can get your money back... IF you act quickly.*” The reality is that many victims do not find out they were scammed quick enough for financial institutions to initiate any kind of account freezing or recovery efforts on their behalf. The average time between a scammer fraudulently obtaining these prepaid/gift card numbers and the funds being redeemed on the card is mere *minutes*.¹ Governmental sources tell you to file reports, notify the bank, and call the gift card companies to explain your situation. This is a fool’s errand.

¹ See various news articles accessible online reporting on various prepaid and gift card scams and how these scammers operate, such as [WDSU 7 in New Orleans](#).

Scammers have exploited holes in the entire payment ecosystem—from financial institutions to retailers to the customers both these entities serve. The details and methods may vary, but the anatomy of a gift card scam is essentially the same. Scammers use a variety of tactics to coerce and manipulate their victims into moving their own money out of the bank and loading their funds onto various prepaid and gift card products from which they can easily facilitate the theft of their victim’s funds. This process creates a safe distance between the criminal and the crime, as these cardholder transactions are unmonitored or handled in separate departments of a retailer or by a third-party service provider altogether. Whether by using these cards for merchandise, cash, or discrete payments to a third-party, scammers quickly turn their ill-gotten gains into a seemingly legitimate transaction long before their victims even realize what has happened to them. Scams are harmful to the entire payment ecosystem, but it is the victim—the consumer—who pays the price.

Current banking regulations and federal consumer protection laws fail to adequately address and prevent consumer harm caused by scams in numerous ways. For example, banks are widely considered the “first line of defense” in protecting an individual’s account from suspicious activity and fraud. Most financial institutions advertise some form of “constant fraud monitoring” protection for their customer’s accounts. Despite evidence of the magnitude of financial damage that scams create for banking clients, an individual’s accounts lack monitoring for suspicious and unusual spending behavior tied to the use of the accountholder’s debit card. Financial institutions may or may not have sufficient resources with which to properly address this type of security issue internally; however, when viewed under the scope of current EFTA regulations, there may be a broader reason for the lack of behavioral monitoring by banks: any transaction made by the accountholder (or by someone at the direction of the accountholder) with an identifiable account access card is generally deemed an authorized transaction.²

While there are exceptions to this policy (specifically, fraudulently obtained account information, robbery, and physical duress), banks are under no legal obligation to reimburse its customers for transactions they themselves authorized—fraudulently induced or not. Scammers are able to exploit this account security vulnerability and the issue of consumer liability whole-heartedly. Without an intervening party (such as the bank), consumers are left on their own with a highly predatory individual(s) whose ultimate intentions are to steal their money. These types of fraudulently induced transactions are viewed more in line with “buyer’s remorse” than the *result of an exploitive criminal act*, leaving consumers with no protection from the substantial monetary harm befallen them.

² See Time’s March 2024 article, “*Banks Aren’t Doing Enough to Protect Customers from Scams*” accessible [here](#).

Similarly, retailers are very aware of organized retail crime and its far-reaching impact on customers, store inventory losses, safety and security, and profitability metrics. Prepaid and gift card fraud is a relatively easy way for criminals to fund money-laundering activities. Many retailers have taken notice of the prevalence of prepaid/gift card scam purchases within their stores and (as evidenced by various business websites) are taking “an active role” in helping consumers avoid scams. Notably, large prominent retailers like Target and Walmart have claimed to have increased in-store warning signage and engaged their personnel in scam prevention efforts. These efforts may have proven successful in stopping some customers from purchasing gift cards for scammers, but the FTC data on gift card fraud suggests these successes are the exception—not the norm. Signage that is not clearly visible is unarguably futile in functioning as an adequate warning to consumers and the ability for store personnel to spot a customer under the spell of a scammer depends on a whole host of variables that can be (understandably) outside of their control.

The U.S. market for prepaid and gift card sales is stout and robust.³ Retailers smartly rely on these sales to increase customer loyalty, receive cash injection infusions, and make future sales projections. Whether a customer buys a gift card for their nephew for his tenth birthday or for a person claiming to be with the IRS who is willing to settle a tax lien with payments via gift cards, retailers benefit from the sale. Funds loaded on a merchandise gift card are recorded as a liability in accounting ledgers and profits are not earned until the funds are redeemed through future merchandise purchases. The rapid turnaround time between a scammer receiving stolen gift card numbers and the funds on it being redeemed results in quickly realized earnings and less shrinkage for a retailer. Scammers exploit real-time payment processing networks, the generally understood nature of gift card giving, and the relative anonymity of gift card transactions. Retailers collect an abundance of information about customers from each transaction, but do not standardly use technology to monitor the funding of a physical gift card in one place and the speed with which it is redeemed online in another location—often a major indicator of gift card fraud.⁴

In the aftermath of a scam, consumers are denied financial protections under the EFTA when the (“closed loop”) gift card purchase they authorized is fraudulently redeemed. From the retailers’ perspective, they properly sold and delivered goods as promised and these merchandise cards are treated essentially as cash. So, they are entitled to decline to help customers with their scam losses or, perhaps even worse, to receive law enforcement,

³ See Payments Journal’s August 2023 reporting on prepaid and gift card sales data from BHN and NAPCO [here](#).

⁴Numerous software and technology blogs (such as this [blog published by Fingerprint](#)) indicate the tools for retailers to use to detect gift card scams are widely available. See also reporting in January 2024 on Walmart’s new “Redemption Program” which allows for detection and prevention of gift card fraud [here by Payments Journal](#).

FTC, or FBI ic3 reporting that would document fraudulent gift card usage in their stores. Target Corporation is one prominent retailer frequently mentioned in the news all over the country about its customers being scammed into buying their merchandise gift cards since 2021. Target spokesmen routinely express regret about their loyal customers being scammed into buying Target gift cards; but they refer back to their in-store signage and front-end team scam training as proof of their valuable contribution in the fight against fraudsters.⁵

Using FTC data, it is surmisable that retailers earned nearly a billion dollars from consumer gift card scam losses since 2020. This consumer “societal problem”⁶ does not appear to be subsiding in 2024. Unless operations are conducted in a state where scam warning signage laws have been enacted, retailers (like Target) are under no obligation to enforce its own stated policies on signage and employee intervention training to help prevent scams in its stores.⁷



⁵ Numerous news articles routinely report on consumers being scammed with Target gift cards and Target's response, such as these from [KARE11 news in Minnesota](#) in December 2021, [abc7 news in California](#) in February 2023 and [ClickOrlando.com news in Florida](#) in February, 2024.

⁶ See news article entitled “*Fraud Victims Demand Chase Bank Do More*” by [WXYZ 7 news in Detroit](#) from February 2023.

⁷ Photographs taken at my local Target store on July 10, 2024, demonstrate a lack of clearly visible signage on the gift card rack and no signage at the registers to warn customers about gift card scamming and fraud despite Target Corporation's claims to the have done so (see Footnote 5). See also Target Corporation's website page on fraud and scam prevention [here](#).

Scammed consumers are deprived of liability protections offered by prepaid card companies or the Visa / Mastercard networks these cards run on because of a loophole in current consumer protection laws: the failure to register the (“open loop”) prepaid card with an online account before their funds are stolen by scammers. These prepaid card companies (backed by larger banks) are allowed to skirt consumer financial protection laws by hiding behind the “no refund” policies of stolen or lost gift cards and the exclusion of certain anonymous transactions made against the funds on the card. As evidenced by numerous state and federal class action lawsuits nationwide and customer complaints filed with the Better Business Bureau, two well-known prepaid card service providers (InComm Financial Services and Green Dot) are frequently accused of failing to provide refunds for unauthorized transactions and/or allow customers access to their funds during the dispute process in direct violation of consumer protection laws.


In servicing the Visa Vanilla Gift Card, InComm requires cardholders to fill out “transactional dispute forms” before error investigations begin. This presents a major difficulty for scammed consumers when time is of the essence for hopes of any kind of financial recovery. InComm’s cardholder policy states that refunds (for any reason) must come from the merchant who accepted the transaction.⁸ The merchant may or may not approve the refund depending on if the cardholder’s identity can be verified against its online transactional records. Despite being presented with police reports documenting a crime, prepaid / gift card service providers usually view scam transactions as authorized because the cardholder supplied the card information “willingly” to a third party.⁹ Chargebacks then get extremely murky for both the prepaid card company and the merchant involved as first-party fraud is evidently very common. Scammers rely on this and (again) have successfully maintained sufficient distance between themselves from their crime, making it nearly impossible for consumers to seek reimbursement for their stolen funds.


The most egregious part about prepaid / gift card scams is that each of these large, powerful industries (banks, retailers, and prepaid card companies) acknowledge consumer fraud and scams are rampant but abdicate any responsibility they have in meaningful consumer protection measures and are simply not incentivized to change. In fact, these

⁸ For example, see Vanilla Visa Cardholder Agreement for cards beginning with 409750 accessible online [here](#).

⁹ Under Reg E, an unauthorized EFT does not include transfers initiated by a person who was furnished the access device to the consumer’s account by the consumer. However, according to the CFPB’s *Electronic Fund Transfers FAQs* updated on June 4, 2021, “EFTs initiated using account access information obtained through fraud or robbery fall within the Regulation E definition of unauthorized EFT. See Comment 1005.2(m)-3.” These two statements are generally confused by prepaid card service providers, who seem to prefer the less protective version of the two scenarios for error resolution processes in which a cardholder was scammed.

sectors actively lobby *against* any new measures which seek to enhance and strengthen consumer protection for scams,¹⁰ all the while earning revenues and shifting blame to defrauded consumers as “willing participants” in the crime that was perpetrated against them.¹¹ One notable online banker’s forum had participants engaging in a lively discussion about dealing with transaction disputes from scammed bank customers under Reg E.¹² One of the participants suggested that scammers are “coaching the duped cardholders” on how to get their money back from the banks,¹³ while another referred to a banking customer as “stupid” for falling for a fake website scam in the first place.¹⁴


Re: Reg E Dispute and Scams
[travelgirl1](#)
#2218011 - 07/19/19 03:02 AM



JacF
MOD
Power Poster
Joined: Nov 2001
Posts: 6,719
PA


I suspect that the scammers are coaching the duped cardholders into filing fraud claims after purchasing the gift card purchases. I would not be surprised if we continue to see more of these types of claims.

We had a similar situation recently. The only difference for us is that the customer adamantly insisted that he did not complete the purchase. We involved the local police, and the customer maintained his story with them, too. We got video from the store, showed the customer pictures of him purchasing the gift cards, took back his provisional credit, and closed his account.

Oh, and he's also being charged for filing a false report...

[Return to Top](#)


Re: Authorized or Not?
[ricarey](#)
#2264558 - 01/11/22 02:24 PM



Compliance NABW
Diamond Poster
Joined: Oct 2015
Posts: 1,669
PA


Originally Posted by ricarey

And just who provided that number and info - the consumer. You can give away the bank if you choose to - most choose not to give away more than what is already required.

Yes, due to fraud. Just like they provide the card if somebody points a gun at them.

[Return to Top](#)


Re: Authorized or Not?
[1995Banker](#)
#2264565 - 01/11/22 03:36 PM


ricarey
10K Club
Joined: Jul 2001
Posts: 83,914
Galveston, TX

The consumer willingly used the fake website - nobody was holding a gun to their head.

Were they stupid, yes.

Does Regulation E protect against such stupidity - no.

Maybe their card issuer rules might cover it if they ordered merchandise that has failed to show up, for example, but we are not talking about card rules. They authorized the charge and that is really the end of the story as far as Regulation E is concerned.

The opinions expressed here should not be construed to be those of my employer: [PPDocs.com](#)

¹⁰ For example, see Consumer Finance Monitor, “Democratic Senators Send Letter to Federal Banking Agencies” notes ABA’s 2022 objection against shifting liability to banks for fraud on P2P platforms, accessible [here](#).

¹¹ See ABA Banking Journal’s April 2023 article entitled, “Americans Blame Themselves for Falling for Real-time Payment Scams” accessible online [here](#). The FICO study promotes a dangerous self-serving bias in the banking industry that may thwart standardized utilization of more costly advanced technologies (such as real-time payment monitoring) for additional (and less costly) awareness and warning messaging in response to bank customer scams.

¹² See BankersOnline.com forum from July 2019 entitled “Reg E Dispute and Scams” accessible [here](#).

¹³ *Ibid*.

¹⁴ See BankersOnline.com forum from March 2018 entitled “Authorized or Not?” accessible [here](#).

While this site certainly appears to be an off record “water-cooler chat” environment for banking professionals, such rhetoric and mindsets exemplify the deepened resolve banks have against investigating fraudulently induced transactions and reimbursing customers for their legitimate losses. Scammed consumers are particularly vulnerable and should have a reasonable reliance that their bank will act in their interests. This is simply not so.

Fraud, as a deceptive act, has been long held in numerous areas of the law to be ‘a spoiler of consent’ and, by its very nature, an unfair and unlawful act. Fraud induces a person into a situation whereby he/she cannot reasonably avoid injury from taking a particular action because of the interference with their ability to effectively make decisions or to choose to take another course of action to avoid injury. Scams are rooted in fraud and perfected by theft. Consumers are subjected to undue influence and actively coerced into purchasing unwanted products (such as prepaid / gift cards) by a third party whose intention is to avoid detection and steal their money. Consent, in this instance, is understood as a payment authorization for a transaction.

While significant steps have been taken to protect consumers from fraudulent transactions initiated by a third party, many consumer protection laws stop short of providing much needed protection from scams. The manipulative and coercive tactics used by a third party to trick an account holder into providing his account access information from which funds are stolen are the very same used to trick an account holder into purchasing prepaid/gift cards from which funds are stolen. The end result is the same. The nuance is who pressed the button. Consumers are treated unfairly and deprived of much needed assistance and vital consumer protections when they are held solely accountable for actions taken as an unwitting victim of a criminal— on the front and back end of these transactions.¹⁵ The defrauded consumer’s authorization is still held as valid even though he/she would not have made a purchase but for a fraudulent third party’s deceit.

Without having too much inside knowledge, it can safely be presumed that scams are extremely complicated to sort out. Acts of collusion, first party fraud, and other improprieties—if unchecked—can cause undue harm to the multiple merchants and financial institutions involved in making and completing one single financial transaction. In cases of prepaid / gift card scams, maintaining the integrity of the payment ecosystem have clearly outweighed the need for consumer protection. Creating public awareness around the problem is important and can facilitate educational measures for consumers to help themselves avoid harm. *But is an online awareness campaign an adequate stand-alone*

¹⁵ See the FINRA Investor Education Foundation collaborative study released in 2022, “*Blame and Shame in the Context of Financial Fraud*” accessible online [here](#).

preventative measure if there are no metrics to identify whether consumers actually receive these types of messages? Industries involved in scam public awareness campaigns generally communicate this information to customers in the form of blogs posted on their websites. Consumers, however, routinely use apps on their phones in transacting with retailers and banks. This kind of important communication attempt can get lost if a customer does not know he/she should be looking for it. Without other methods to ensure communications actually reach consumers, efforts to “generally” relate awareness and warning fall woefully short.¹⁶ Conveying the financial liability (and subsequent fallout) of a scam onto the consumer without holding the larger industries accountable for the activities, products, and services each provide contributes to substantial injury for consumers and, as such, is systematically unfair.

- Banks have an ethical and legal responsibility to their customers, but “constant fraud monitoring” does not include the real-time detection of suspicious and unusual account activity that would allow them to see customer account draining through multiple transactions in repetitious amounts in a relatively short period of time.
- Retailers are not required to post in-store scam warning signs in most states or monitor gift card funding beyond basic transactional levels, but they profit off of their customers’ fraudulently redeemed gift cards.
- Prepaid card liability protections are given upon account enrollment and verification processes, but scammers keep their victims focused on a fictitious problem so the stolen account numbers can be passed on to other associates for immediate use.
- Prepaid card service providers frequently fail to reimburse scammed cardholders for fraudulent transactions against their account, choosing instead to believe that a cardholder “willingly” gave their card information to another person to use—even when presented with a police report documenting the crime.

Substantial injury is quantified by ‘a small amount of harm to a large number of people’ or ‘a significant amount of harm to a small number of people.’¹⁷ Respectfully, consumers have been at both ends of that point for several years now. Current laws and regulations simply do not address the monetary harm born by scammed consumers—harm that cannot be reasonably avoided without meaningful assistance and intervention from the other key industry sectors inadvertently involved in the carrying out of scams. This creates a direct conflict of interest between vulnerable consumers and industries who serve them—who stand to either financially benefit from their own customers’ losses or to limit their

¹⁶ See ABA Banking Journal’s April 2023 article entitled, “Americans Blame Themselves for Falling for Real-time Payment Scams” accessible online [here](#).

¹⁷ See Federal Trade Commission Act, Section 5: Appendix, Unfair or Deceptive Acts or Practices, “Accessing Whether an Act or Practice is Unfair,” pg. 7, accessible online [here](#).

exposure in absorbing the financial loss themselves. These practices are the antithesis of consumer protection, leaving defrauded consumers in a “no-win” position.

The FTC contends that most financial crimes go unreported by victims out of fear, embarrassment, or shame for having been conned, even though victims’ financial losses may be substantial. Local law enforcement cannot easily arrest a suspect who is unknown, outside of their jurisdiction, and virtually untraceable online. Retailers and financial institutions are interested in mitigating their own losses where they can—protecting assets, profitability, and shareholder equity—and are not interested in shouldering any more liability than they absolutely have to these days. Nevertheless, enhanced *financial protections for scammed consumers are desperately needed* and, if granted, would lead to more collaborative efforts to keep consumers safe. Retailers, prepaid card companies, and banks would be compelled to implement proactive meaningful measures toward the detection and intervention of fraudulent activities— if nothing else but to mitigate their own risk and exposure to liability. Further, more scam victims may be willing to report these crimes to local law enforcement if by doing so they were afforded any kind of help to avoid financial devastation. In turn, more crime report data would be available from which to investigate patterns and shut down these organized crime rings. As it stands, consumers are left on their own to deal with experienced, well-organized criminals who continually divest them of their hard-earned money, while large powerful industries stand by and let it happen.