How Policymakers Can Prevent Gift Card Scams

By Becca Trate | December 12, 2022

Gift card scams are on the rise. Scammers have relied on predatory tactics, emotional stories, and product tampering to steal nearly $450 million from unsuspecting Americans in the last three years alone, and the trend shows little signs of slowing. Consumers from all age groups, but especially older consumers, are burdened with heavy loss and little recourse if they fall victim to a gift card scam. Policymakers in the United States should expand the Electronic Fund Transfer Act (EFTA)—a law that establishes rights and responsibilities for a variety of electronic payment systems—to include stronger consumer protections for gift cards; encourage gift card issuers and businesses to introduce stronger security features for gift cards; address gift card fraud as an international issue; create more effective solutions; and launch a data-sharing pilot that increases information on scams and helps merchants and gift card issuers implement realistic solutions to prevent future scams.

INTRODUCTION

Gift cards are popular among consumers because they are easy to use in-person or online, can be purchased almost anywhere, and allow the recipient to spend on products of their choice. But these qualities make them equally attractive to scammers, and gift cards represent one of the most common avenues criminals use to defraud consumers.[1]

Americans reported more than $233 million in losses related to gift card fraud in 2021.[2] This number will only continue to grow if policymakers,

retailers, and gift card issuers fail to take action to protect consumers. This report outlines practical solutions that policymakers should adopt to address growing levels of gift card fraud. They include:

- Congress should update the EFTA to treat gift cards like debit cards, which would encourage companies to implement proven security features to protect against liability.
- The FTC should modernize its education campaign by working with industry to introduce warning messages on point-of-sale devices to increase awareness of gift card scams.
- The FTC should launch a data-sharing pilot program designed to increase the number of data contributors to its Consumer Sentinel Network—a repository of consumer complaints—to better track gift card fraud.
- The FTC should break out data for payments by virtual, mobile, and physical gift cards on Sentinel.

GIFT CARD FRAUD

Nearly one-fourth of all consumer fraud reported in the United States involving money loss is connected to gift cards.[3] According to the Federal Trade Commission (FTC), scammers gravitate towards gift cards because they are easily accessible to both scammers and victims, offer fewer consumer protections than other payment methods, and allow fraudsters to quickly access, transfer, or spend the funds while remaining anonymous.[4]

There are two categories of gift cards—open-loop gift cards and closed-loop gift cards. Open-loop cards, such as Visa or Mastercard-branded gift cards, run on payment card systems and are redeemable anywhere the associated card brand is accepted. Open-loop cards typically have a small fee to activate, paid at the time of purchase. Closed-loop gift cards are gift cards that are only redeemable at the associated merchant or retailer listed on the card. Closed-loop cards are usually free to activate and generally hold only the value listed on the card and cannot be reloaded.[5] The FTC found that scammers tend to prefer closed-loop gift cards because they are easily obtained by consumers and because closed-loop gift cards valuing less than $2,000 are exempt from the Financial Crimes Enforcement Network's (FinCEN) anti-money laundering reporting requirements.[6] The FTC found that Target-branded gift cards accounted for the highest total loss ($35 million) reported to the FTC in the first nine months of 2021.[7]

There are several different kinds of gift cards. Physical gift cards are actual cards, typically swipe cards that use a magnetic strip and bear the gift card number and associated pin, if necessary, and are loaded with a value. The value may be pre-determined or chosen by the purchaser. Physical gift cards can often be used online, as well, by entering the card number and

pin at the point of purchase. Digital gift cards, or e-gift cards, are electronic gift cards. They have no physical component and typically include just the card number and pin, if necessary, but can often be printed out and used in-store or online. Finally, mobile gift cards are gift cards that can be loaded onto a mobile wallet. They may or may not have a number associated with them but can be used anywhere the gift card and mobile payment is accepted, both in store and online.[8]

Common Gift Card Scams

Imposter scams were the most common scam reported to the FTC in 2021 that involved gift cards.[9] These involve scammers contacting victims, usually over the phone, and impersonating a trusted entity, such as government agencies or officials, utility providers, tech support workers, or well-known businesses. The scammer will claim the victim owes a debt or needs to submit a payment. The scammer tells the victim they must pay with a gift card immediately or they will suffer severe consequences. Another common imposter scam features the scammer impersonating a consumer's loved one in distress, using details about the victim and their loved ones from social media to corroborate their story.[10] The perpetrator of imposter scams could be anywhere in the world.

Scammers stress urgency when perpetrating an imposter scam and will typically instruct victims on where to purchase the cards, often sending victims to multiple retail locations to avoid suspicion and detection by store employees. Scammers will often keep victims on the phone for the entire duration, to prevent a victim from calling another person for assistance and may even feed a victim information to tell concerned employees. Once the gift card is active, scammers will ask the victims to provide the card's 16-digit number and pin, if applicable. As soon as a scammer receives this information, they will steal any funds loaded onto the card. The value is stolen by selling the card information to a third-party gift card trafficker to liquidate the card's value, using the card value to purchase items to be resold, transferring the value from the card into a different digital asset, or using another method to empty the card's value.[11]

Gift card payment scams are very similar to imposter scams. Gift card payment scams direct the victim to use a gift card to pay for something that seems legitimate, such as a parking ticket, bill, consumer product or service, or to secure a refund.[12] Scammers may create fake websites that mirror real payment sites to perpetuate this scam or ask consumers to pay directly over the phone.[13] Methods behind gift card payment scams change rapidly.

In addition to imposter scams, which are mostly conducted remotely, some scammers will physically tamper with cards in retail stores before consumers purchase them.[14] These are called zero-balance card scams. In these scams, fraudsters discreetly open gift card packages, remove the security tape from cards, and collect numbers. The scammer will digitally

monitor the numbers and drain the value after someone purchases and activates the card.[15] Thus, anyone purchasing a card could easily become a victim, and they may not even realize they have become a victim until the recipient of the gift card discovers the empty balance on the card and notifies them.

Another type of common in-store scam uses credit card skimmers. Card skimmers are electronic devices that collect payment information stored on the magnetic strip of a payment card when the card is swiped. The data is then transferred wirelessly or downloaded by the scammer. Overlay skimmers, usually found on ATM or point-of-sale (POS) machines, sit directly on a credit card reader, and look like an original device.[16] More sophisticated skimmers are attached to the card reader's internal wiring and are not visible to the purchaser. These are often found at fuel pumps or on machines that are largely unmanned or away from employees because scammers can discretely install them more easily.[17] Scammers can use collected credit card numbers to buy gift cards, or can collect information from gift cards when the card is purchased or used.

Monetizing Gift Card Fraud

Once fraudsters receive a gift card, there are several ways they can turn the card into usable currency. One of the simplest methods is to use the card to buy products, or other gift cards, that can be resold. However, this method may require a runner to use the cards quickly and collect purchased goods, or a delivery address to send goods purchased online.[18] Scammers may also use online gift card conversion facilities or physical conversion kiosks to exchange cards directly for cash.[19]

Scammers can also liquidate the value of gift cards on online gift card exchange markets. Formal resale markets operate through specific online platforms to purchase gift cards for less than the face value and resell them directly to consumers at a discounted price, or connect consumers to sell directly to each other. [20] These platforms automatically check a card balance before sale to prevent scams, and specific platforms maintain consumer protection practices.[21] For example, CardCash, the largest formalized U.S. gift card resale market, maintains a consumer refund period and boasts several anti-fraud measures, such as seller registration and card vetting to prevent fraudulent cards from being sold of its platform.[22] However, these measures do not stop scammers from liquidating gift cards on these gift card exchange markets.

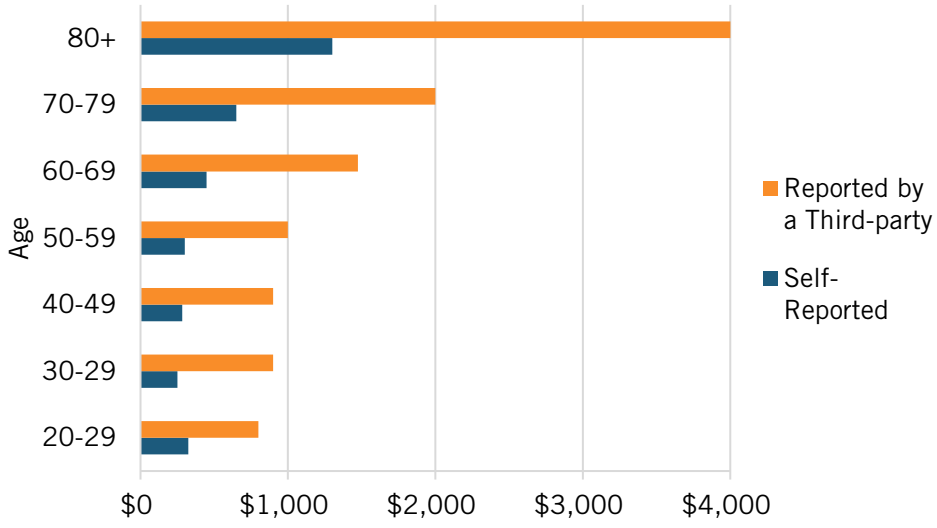
Scammers also liquidate cards on informal resale markets. These markets operate through social media, on third-party marketplaces such as eBay or Craigslist, or the dark web.[23] Gift card holders use these platforms to list gift cards for sale and sell directly to consumers.

Victims of Gift Card Scams

More Americans are being targeted by gift card scams than ever before, and research shows scammers will target anyone, regardless of age. AARP, an advocacy group representing Americans ages 50 and older, reported one-third of all U.S. consumers had been targeted by a gift card payment scam at least once, and the number of victims is growing.[24] Another survey of American consumers conducted by the AARP Fraud Watch Network in 2022 found around a quarter of respondents were victims of zero-value cards scams.[25] In 2021, victims in the United States self-reported almost 70,000 instances of gift card payment scams, increasing from 38,400 scams reported in 2019, and 43,200 reported in 2020.[26]

The total monetary losses from gift card fraud reported to the FTC grew to over $233 million in 2021, up from $116 million in 2020 and $99 million in 2019.[27] The FTC estimates that the total value of losses to American consumers may be much higher. Victims often underreport or do not report monetary losses when reporting scams due to embarrassment and shame. In 2020, the median self-reported monetary loss for all ages was $300. In contrast, the median loss reported on behalf of a victim by another individual was $1,000.[28] When a third party such as a financial institution or retailer reported on behalf of a victim, the median monetary losses were $4,000 for consumers ages 80 and older, $2,000 (ages 70-79), $1,474 (ages 60-69), $1,000 (ages 50-59), $900 (ages 40-49), $900 (ages 30-39) and $800 (ages 20-29).[29]

Figure 1: Median monetary losses from gift card fraud in the United States in 2021, by reporter



In addition, the frequency and accuracy of reporting monetary losses also decreases with age. Adults ages 60 and above were 28 percent less likely to report scams if they lost money as compared to adults below the age of 60.[30] Adults ages 60 and above also reported higher overall losses and

were likely to report gift cards as the payment method when reporting scams.[31]

Data Collection on Gift Card Scams

The FTC collects and analyzes data on gift card scams through the Consumer Sentinel Network (Sentinel), a centralized tool managed by the FTC to provide federal, state, and local law enforcement agencies with access to reports from consumers regarding fraud and scams. Sentinel receives data on consumer fraud complaints reported directly by consumers to the FTC and from 45 data contributors, including federal agencies, state agencies that collect consumer complaints, state-level attorneys general, consumer groups like the Better Business Bureau and AARP, and a handful of businesses.

However, Sentinel suffers from incomplete data because consumers underreport scams overall, and not all scams reported to law enforcement or state agencies are reported to the FTC. First, before any information is reported to Sentinel, consumers must choose to report the fraud. While around half of adults who become victims of fraud will complain to their loved ones, fewer than five percent will eventually report the fraud to a government organization or consumer protection group such as the Better Business Bureau.[32] But, even when a fraud victim does report, the data still may not be included in Sentinel's dataset. Victims must report to a data contributor to be included, such as a local law enforcement agency, a consumer protection group, or directly to the FTC. If the victim reports to a state agency, attorney general's office, or local law enforcement agent that is not a data contributor, the case is not reported to Sentinel.[33]

The FTC cannot accurately track fraud without knowing what fraud occurred, nor can it implement effective and responsive policies. Law enforcement agencies cannot effectively investigate fraud, prosecute bad actors, identify victims, provide restitution, and educate the public about common scams without relevant, up-to-date information on scams.

CURRENT POLICIES PROTECTING CONSUMERS FROM GIFT CARD FRAUD

Scammers prefer gift cards because they are accessible to consumers and easy to convert into currency through purchases or resale. Gift cards also lack consumer protections and regulations that apply to other payment methods, meaning they are largely untraceable and unrecoverable once the fraud occurs. Finally, closed-loop gift card purchases do not require reporting or tracking by financial and government agencies, allowing scammers to receive large sums of money undetected.

Government Policies

While federal and state laws protect consumers from gift card expiration and inactivity fees, with special reporting requirements to prevent money

laundering, they do not protect consumers against misuse or unauthorized charges. This makes gift card protections significantly different—and weaker—than protections for credit and debit cards.

Credit CARD Act

The Credit Card Accountability and Responsibility and Disclosure Act of 2009 (Credit CARD Act) amended the Truth in Lending Act to protect consumers from unfair credit card practices by requiring greater transparency in credit card terms and conditions and contained special provisions for both open and closed-loop gift cards.[34] The Credit CARD Act introduces special requirements for gift cards, including fees and expiration dates disclosures, limits on gift card inactivity fees, and minimum periods before a gift cards can expire.

The Act also amended the Electronic Fund Transfer Act (EFTA), which aims to protect individual consumers engaging in electronic fund transfers, to account for the use of gift cards. Generally, the EFTA prohibits merchants from levying fees to the gift card holder, except in limited circumstances.[35] Changes also ensures that the EFTA does not preempt any state laws addressing fees or dormancy if the state laws provide greater consumer protections than the EFTA.[36]

The Credit CARD Act did not extend all provisions of the EFTA that apply to credit and debit cards to gift cards. Notably, consumers do not have the same protections for misuse or unauthorized charges on gift cards.[37] If a gift card is stolen from someone, for example, the consumer has no recourse beyond filing a police report, like stolen cash. In contrast, the EFTA limits liability for a consumer if someone uses a lost or stolen debit or credit card to make fraudulent purchases. The law also protects consumers if someone steals a card number without stealing the physical card.[38]

Bank Secrecy Act

Congress enacted the Bank Secrecy Act (BSA), also known as the Currency and Foreign Transactions Reporting Act, in 1970 to prevent money-laundering. Following a 2011 rulemaking, provisions of the BSA now apply to the sale, issue, and redemption of gift cards and other stored-value cards and requires reporting of specific card sales to the Financial Crimes Enforcement Network (FinCEN), a bureau of the Department of the Treasury that collects information on financial crimes like money laundering. [39] For a gift card transaction to require reporting to FinCEN, the purchaser must spend $2,000 on a single gift card in a day or spend $10,000 on gift card purchases in a single day.[40]

Closed-loops cards are generally considered low-risk for money laundering by the Department of the Treasury, since they can only be used in a specific retail environment and have no surrender value.[41]

State Level Protections

States also have different protections for gift cards, but generally, protections cover fees to use the card, dormancy and expiration, and abandonment, and do not include protections in the case of fraud or unauthorized use.[42]

Consumer Education

The FTC, retailers, and consumer protection groups work together to reduce the level of gift card fraud through consumer education. The FTC's primary gift card fraud campaign, "Stop Gift Card Scams," partners with retailers to put signs around the point-of-sale or check-out area to remind consumers about gift card fraud. Retailers also train their employees to spot potential scams and help shoppers who may be under distress or are acting out of turn.[43] Understanding the signs of someone falling victim to gift card fraud is effective at stopping scams. AARP found that more than half of people who reported a third-party intervention were able to avoid losing money to a gift card scam.[44]

The FTC also maintains other education campaigns, such as "Pass It On," which partners with public libraries to educate the public about different types of scams and fraud.[45] AARP also maintains a dedicated help line, various web pages, and a watch-dog alert system to inform consumers about scams and to assist consumers who fall victim to scams.[46]

Technological Interventions

Retailers have also taken a role in protecting consumers by using technology to identify and flag potentially fraudulent patterns involving the use of gift cards. Both traditional and e-commerce retailers have access to vast datasets about their consumers' purchase history, shopping habits, and behavior.[47] Data allow retailers to make predictions about consumer future behavior and purchases and can help retailers detect fraud.

While data is not a magic bullet to detect or prevent fraud, it does provide a starting point for investigators. Data analytics identify anomalies; investigators then determine if fraud occurred.[48] Analytics cannot yet replace fraud auditing but using data analytics allows investigators to identify fraud more quickly and prevent greater fraud.[49] Indeed, in an affidavit filed in Arkansas as part of a gift card forfeiture case, Walmart revealed its technology had identified more than 10,000 suspicious transactions valued at more than $4 million. Walmart was able to freeze assets related to the fraudulent cases and help the victims after they had been scammed.[50]

In addition to data analytics, retailers are increasingly using artificial intelligence (AI) in their fraud prevention divisions.[51] While retailer's AI systems are getting more sophisticated in predicting and preventing return, product loss, and other retail fraud, limitations still exist around gift card

fraud since algorithms best identify suspicious activity after it has occurred. Still, moving towards machine learning-based systems can be especially effective for continued gift card fraud detection.[52] Machine learning-based AI systems can adjust to the dynamic nature of the fraudulent activity and detect anomalies at the first arrival better than rules-based programming.[53] The largest gift card technology providers, BlackHawk and Incomm, use advanced AI systems that can detect and alert stores of fraud, but this happens after the sale. To prevent scams from succeeding, retailers and banks must detect fraud in real-time and intervene before the victim provides the gift cards to the scammer.[54]

Card Security Features

Although credit and debit cards look like gift cards, they are very different. Gift cards represent the most basic type of card, lacking almost all security features. Even when digital or enabled for mobile wallets, gift cards are not encrypted, and physical cards have the magnetic strip and relevant card information and pin printed directly on the card.

On the other hand, credit and debit cards have security features built directly into the card, such as numberless cards, chip-and-pin security, and tap-to-pay near-field communication (NFC) tags. Security features help to reduce credit card fraud, especially related to skimming. The introduction of the chip and pin-equipped card, or chip card, reduced counterfeit card fraud by 76 percent in three years, according to a study by Visa.[55] This reduction occurred because it is practically impossible to “skim” a cardholder’s information when the chip is used, since the information is encrypted. This is also true for NFC tap-to-pay cards and NFC credit cards used in mobile wallets.[56] The security benefits and uses of chip-enabled cards have led issuers to phase out the magnetic stripe entirely. Mastercard plans to remove the magnetic stripes for all credit and debit cards by 2033.[57]

Similarly, multinational bank Banco Santander claims that numberless cards, which store all data on the chip and do not have any numbers present on the card, reduce the risk of fraud by up to 90 percent.[58] Consumers must access their credit card numbers through an online system or connected mobile wallet to make online purchases. Users set up mobile wallet access when they activate the card. They can also add access through a card’s mobile app at a later date.

RECOMMENDATIONS TO IMPROVE CONSUMER PROTECTION FOR GIFT CARD FRAUD

Since the FTC’s “Stop Gift Card Scams” campaign launched in 2020, the total losses from gift card fraud have doubled, growing year-to-year since the FTC began collecting data.[59] To help curb fraud, policymakers should focus on proactive measures that make gift cards less attractive to

scammers, decrease the losses associated with gift card fraud, and better protect consumers from fraud overall. Specifically:

- Congress should update the EFTA to treat gift cards like debit cards, which would encourage companies to implement proven security features to protect against liability.
- The FTC should introduce alerts on point-of-sale systems to increase awareness of gift card scams at the point-of-purchase.
- The FTC should launch a data-sharing pilot program designed to increase the number of data contributors to Consumer Sentinel network.
- The FTC should break out data for payments by virtual, mobile, and physical gift cards on Sentinel.

Extend Consumer Protections in the EFTA To Gift Cards and Promote Use of Proven Security Features

Congress should update the Electronic Funds Transfer Act (EFTA) to make gift card issuers, or associated merchants, liable for unauthorized charges on both open-loop and closed-loop gift cards. Currently, consumers are protected from unauthorized use on debit and credit cards under EFTA, but consumers still bear most of the cost of gift card fraud. Making issuers and merchants liable for unauthorized charges would incentivize them to implement effective security features on gift cards to reduce fraud or discontinue offering them if the cost is too high.

Shifting the liability to merchants has been effective in improving credit card security and reducing fraud. In 2015, major U.S. card issuers switched liability for merchant-related credit card fraud from the issuer to the merchant for any transaction from a card with an electronic chip.[60] This encouraged merchants to make the switch to more secure chip-and-pin card readers. The switch went into full effect in April 2021, and chip card use has grown tremendously as a result.[61] Analysts estimate that the transition from magnetic swipe to chip cards cost upwards of $8.6 billion across the United States, but most of the cost was incurred by replacing the machine card readers with more expensive chip-readers.[62] The extra cost to produce chip cards as compared to magnetic swipe cards is generally around $1.[63] Cards enabled for contactless payment cost around the same as magnetic swipe cards, while mobile or digital gift cards are essentially costless to produce.[64]

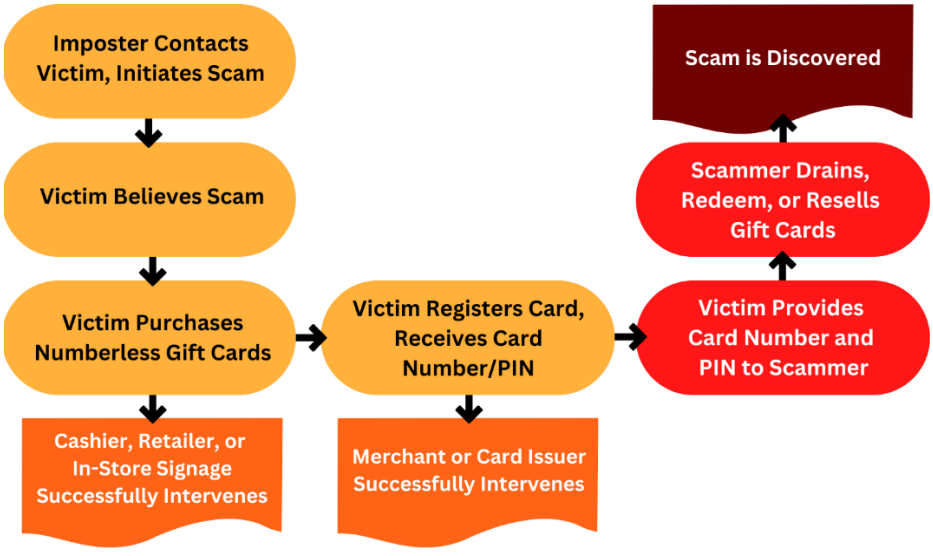
Despite the benefits of chip-and-pin and numberless cards, these security measures have not yet been implemented to stop gift card fraud. In 2022, federal prosecutors in Colorado accused three men of “skimming” nearly 8,000 personal payment card numbers, including gift card numbers, from tampered card readers in Walmart stores.[65] Implementing chip cards could reduce gift card fraud related to skimmed or tampered cards significantly,

without compromising the wide use and acceptance of gift cards by consumers and retailers.

Numberless cards could help the success of impersonation scams, scams that use gift cards for payment, and zero-balance gift cards caused by card tampering. Scammers could not collect the digits and pin from an unsold numberless card. Consumers could purchase, activate, and gift numberless gift cards freely, and numberless gift cards would be ready for in-person use immediately after purchase. But, like numberless credit cards, consumers would need to register to access the card numbers and associated pin to make purchases online. Merchants and card issuers could collect and verify personally identifiable information, such as the consumer's name and phone number, before activating these cards. The process, shown in Figure 2, provides merchants and card issuers an opportunity to intervene and warn customers about gift card scams before they provide information to scammers.

Requiring a verifiable identity to activate a gift card for online purchases would make it much harder for scammers to use anonymity to compromise gift cards. Reducing anonymity in these transactions would make gift card fraud much less attractive to scammers. Moreover, activation portals would provide card issuers a direct line to consumers who may be victims of scams and provide them another opportunity for intervention, such as warning consumers of the risk of sharing gift card numbers and allowing consumers to verify their purchases. Card issuers could also use analytics on activation portals to detect potentially fraudulent activity.

Figure 2: How numberless card can stop imposter scams



Implement Digital Education Campaigns at Point-of-Purchase

The FTC should work with retailers and providers of point-of-sale systems to expand its education campaign beyond physical signs at check-out and around gift card displays and work with the private sector to introduce warnings about gift card scams on the point-of-sale device during the sale transaction. Like physical signs used in the current campaign, pop-ups on the card readers and digital signs, when available, would warn consumers about gift card scams. Warning messages displayed on point-of-sale card readers could require consumers to read and engage as well, like donation, tip, or receipt requests that appear on point-of-sale devices.

Moving away from static signage could help the FTC achieve its goal of increasing awareness of gift card fraud by improving consumer engagement with warnings and information. Many retailers use digital point-of-sale card readers so they may prefer displaying this information on these systems rather than using physical signs.

Improve FTC Data Collection to Better Understand Gift Card Fraud

Retailers already operate innovative solutions that use artificial intelligence (AI) to detect and track gift card fraud, pinpoint accounts and parties associated with the scam, and track spending and monetary losses related to scams.[66] While these systems primarily detect fraud after it has occurred, they still collect a useful amount of information that could benefit law enforcement agencies attempting to build cases. The FTC should collaborate with retailers to access their wealth of data and encourage more retail businesses to join Sentinel as data contributors. To encourage retailers to participate, the FTC should launch a pilot that allows all contributors to access the data collected in Sentinel about gift card fraud instead of restricting access only to law enforcement agencies. Retailers would benefit from this data-sharing pilot by having greater access to reported scams from all data-sharing agencies. Retailers would have information on some of the methods used by scammers, how the scammer started, what was said to the victim, and total gift card denominations that were collected. In-depth information about the type of scams impacting victims could help retailers train employees to better spot and respond to gift card scams in store. More partnerships would also help law enforcement agencies using Sentinel investigate and prosecute fraud by giving greater insight into victims, locations, scams, losses, and potential perpetrators.

Break Out Data for Payment by Virtual, Mobile, and Physical Gift Cards on Sentinel

Currently, fraud data reported to Consumer Sentinel is categorized based on the payment type. Gift cards, regardless of whether they are mobile, digital, or physical, are considered a single payment category. The FTC should break out gift card payments on Sentinel into multiple subcategories to help consumers, researchers, and businesses better

understand the impact of different kinds of payment fraud from gift cards. Making this change would allow interested parties to understand the difference and impact of gift card fraud from virtual gift cards, mobile gift cards, or physical gift card purchased in stores so they can appropriately respond.

CONCLUSION

Current policies related to gift card fraud in the United States overwhelmingly leave consumers to protect themselves from scams-- even as losses grow, scams become increasingly sophisticated, and more Americans suffer. But stakeholders can reduce the prevalence of gift card scams by ensuring stronger protections, better gift card security, and better understanding of the type, scope, and impact of fraud.

All stakeholders, including the FTC, consumer protection groups, law enforcement agencies, retailers, and gift card issuers, should review current policies to understand the gaps that allow exploitation by scammers, and then make commitments to close these gaps with improved data collection, increase gift card security, and better customer education at the point-of-purchase to prevent victimization before it occurs.

These changes would take the onus off consumers to recognize and react to scams while under duress, and instead provide stronger guards that slow down and prevent the passage of information to scammers. Proactive measures like this would also assist lawmakers in finding and prosecuting bad actors through better access to information on scams. Eliminating fraud completely may be an impossible task; nonetheless, gift card fraud is an issue that policymakers, retailers, consumers, and gift card issuers can reduce together.

REFERENCES

1. Emma Fletcher, “Scammers Prefer Gift Cards, but Not Just Any Card Will Do,” Federal Trade Commission, December 8, 2021, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/12/scammers-prefer-gift-cards-not-just-any-card-will-do.
2. Federal Trade Commission, *Consumer Sentinel Network*, (January 23, 2020), distributed by Tableau Public, https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic
3. Fletcher, “Scammers Prefer Gift Cards, but Not Just Any Card Will Do,” Federal Trade Commission.
4. Ibid.
5. Shelly Hunter. “What Are Open Loop Versus Closed Loop Gift Cards?” *Giftcards.com*, April 28, 2017. https://www.giftcards.com/gcgf/open-loop-versus-closed-loop-gift-cards.
6. Financial Crimes Enforcement Network, “FinCEN Issues Prepaid Access Final Rule: Balancing the Needs of Law Enforcement and Industry,“ news release, July 26, 2011, https://www.fincen.gov/news/news-releases/fincen-issues-prepaid-access-final-rule.
7. Fletcher, “Scammers Prefer Gift Cards, but Not Just Any Card Will Do,” Federal Trade Commission.
8. “What is a digital or egift card?”, Kroger, accessed November 12, 2022, https://giftcards.kroger.com/blog/blog-what-is-an-e-gift-card.
9. Federal Trade Commission, *Fraud Reports*, (February 22, 2022), distributed by Tableau Public, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts.
10. Lisa Rowan. “Gift Card Scams Spiked In 2021. Here’s How To Avoid Getting Duped,” *Forbes*, December 9, 2021, https://www.forbes.com/advisor/personal-finance/gift-card-scams/.
11. Fletcher “Scammers Prefer Gift Cards, but Not Just Any Card Will Do.” Federal Trade Commission.
12. Rowan, “Gift Card Scams Spiked In 2021. Here’s How To Avoid Getting Duped,” *Forbes.*
13. Ibid.
14. Susan Tomper, “How to Avoid Gift Card Scams: What to Check before You Buy,” *Detroit Free Press*, December 9, 2021, https://www.freep.com/story/money/personal-finance/susan-tompor/2021/12/09/gift-cards-scam-target-google-play-apple-walmart/6423925001/.
15. “How to Avoid Gift Card Scams: What to Check before You Buy.” *Detroit Free Press*, December 9, 2021. https://www.freep.com/story/money/personal-finance/susan-tompor/2021/12/09/gift-cards-scam-target-google-play-apple-walmart/6423925001/.
16. Federal Bureau of Investigation https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/skimming

17. Federal Bureau of Investigation https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/skimming

18. "Gift Card Fraud: What It Is and How To Stop It," Arkose Labs, accessed November 12, 2022, https://www.arkoselabs.com/explained/gift-card-fraud/.

19. Ibid.

20. Ibid.

21. Scott Denning and Ralph E. McKinney Jr., "The evolution of gift cards in secondary markets and money service," *Journal of International Finance Studies 16*, no. 2 (2016): 27-32, http://dx.doi.org/10.18374/JIFS-16-2.4.

22. "Save with Confidence," CardCash, accessed November 12, 2022, https://www.cardcash.com/guarantee/.

23. Scott Denning and Ralph E. McKinney Jr., "Gift cards in secondary markets and money service," 27-32, http://dx.doi.org/10.18374/JIFS-16-2.4.

24. Sauer, Jennifer. "Gift Card Scams: AARP Survey of U.S. Consumers," April 12, 2022. https://www.aarp.org/content/dam/aarp/research/surveys_statistics/econ/2022/gift-card-scams-survey.doi.10.26419-2Fres.00531.001.pdf.

25. AARP, "AARP Survey: 1 in 3 Adults Hit By Gift Card Payment Scams," *AARP (blog),* April 13, 2022. https://www.aarp.org/money/scams-fraud/info-2022/gift-card-fraud-survey.html

26. Federal Trade Commission (FTC), *Consumer Sentinel Network Data Book 2021,* (Washington, DC: Federal Trade Commission, February 2022), 11, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf; Federal Trade Commission (FTC), *Consumer Sentinel Network Data Book 2020,* (Washington, DC: Federal Trade Commission, February 2021), 11, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf; and Federal Trade Commission (FTC), *Consumer Sentinel Network Data Book 2019,* (Washington, DC: Federal Trade Commission, January 2020), 11, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf.

27. Federal Trade Commission, *Consumer Sentinel Network*, (January 23, 2020), distributed by Tableau Public, https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic

28. Ibid

29. Ibid

30. Federal Trade Commission, Protecting Older Consumers 2020-2021: A Report of the Federal Trade Commission (Oct. 18, 2021), 29 - 30, https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2020-2021-report-federal-trade-commission/protecting-older-consumers-report-508.pdf.

31. Federal Trade Commission, *Age and Fraud,* (February 22, 2022), distributed by Tableau Public,

https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic.

32. Federal Trade Commission, Protecting Older Consumers 2020-2021: A Report of the Federal Trade Commission (Oct. 18, 2021), 29 - 30, https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2020-2021-report-federal-trade-commission/protecting-older-consumers-report-508.pdf.

33. "Consumer Sentinel Network Data Contributors," Federal Trade Commission, July 16, 2013, https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors.

34. "Credit Card Accountability Responsibility and Disclosure Act of 2009," Legal Information Institute, last updated July 2022, https://www.law.cornell.edu/wex/credit_card_accountability_responsibility_and_disclosure_act_of_2009.

35. Roberts W. Sparkes, III et al., "Don't Look a Gift Card In the Mouth: Beware of Liability Under the Electronic Fund Transfers Act" (K&L Gates, April 2016), https://www.klgates.com/Dont-Look-a-Gift-Card-in-the-Mouth-Beware-of-Liability-Under-the-Electronic-Fund-Transfers-Act-04-07-2016.

36. Rebecca S. Reagan and Aaron Thompson, "Credit CARD Act Requirements for Gift Certificates, Store Gift Cards, and General-Use Prepaid Cards," Consumer Compliance Outlook, First Quarter (2013): 4-5, 16-19, https://www.consumercomplianceoutlook.org/2013/.

37. "FDIC Consumer News: What You Should Know About Gift Cards." Accessed April 22, 2022. https://www.fdic.gov/consumers/consumer/news/december2019.html.

38. Michael Scheumak, "Credit Card Fraud vs. Debit Card Fraud: Are You Protected?" *IdentityIQ,* June 20, 2019, https://www.identityiq.com/scams-and-fraud/credit-card-fraud-v-debit-card-fraud-are-you-protected/.

39. "Rules Applicable to Providers and Sellers of Prepaid Access or Stored Value and Gift Cards," Carr Mclellan, accessed November 12, 2022, https://www.carr-mcclellan.com/insights/rules-applicable-to-providers-and-sellers-of-prepaid-access-or-stored-value-and-gift-cards/.

40. "New FinCEN Reporting Requirements for Gift Cards," Secure Payments Systems, accessed November 12, 2022, https://www.securepaymentsystems.com/news/recent-news/new-fincen-reporting-requirements-for-gift-cards. and Lauren Debter, "The Idiot's Guide to Laundering $9 Million," *Forbes,* January 11, 2017, https://www.forbes.com/sites/laurengensler/2017/01/11/gift-cards-money-laundering/.

41. "Rules Applicable to Providers and Sellers of Prepaid Access or Stored Value and Gift Cards," accessed November 12, 2022.

42. "Gift Cards and Gift Certificates Statutes and Legislation," National Conference of State Legislatures, accessed December 6, 2022, https://www.ncsl.org/research/financial-services-and-commerce/gift-cards-and-certificates-statutes-and-legis.aspx.

43. "Stop Gift Card Scams," Consumer Information, December 16, 2020, https://consumer.ftc.gov/articles/stop-gift-card-scams.

44. DeLiema et al, “Exposed to Scams,” https://longevity.stanford.edu/wp-content/uploads/2019/09/ScamTrackerIssueBrief-ExposedToScamsReducedFile.pdf

45. “The FTC and Public Libraries,” Public Library Association (PLA), April 22, 2015, https://www.ala.org/pla/education/onlinelearning/webinars/archive/passiton.

46. “Scam, Fraud Alerts - Protect Your Digital Identity,” AARP, accessed April 22, 2022, https://www.aarp.org/money/scams-fraud/.

47. Maria Monteros, “When online activity soared last year, so did data collection,” *Retail Dive,* August 31, 2022, https://www.retaildive.com/news/when-online-activity-soared-last-year-so-did-data-collection/.

48. Sunder Gee, Fraud and Fraud Detection: A Data Analytics Approach (Wiley Corporate, 2014).

49. Sunder Gee, Fraud and Fraud Detection: A Data Analytics Approach (Wiley Corporate, 2014).

50. Dan Mangan, “How Walmart Thwarted $4 Million in Elder Gift Card Scams,” CNBC, April 4, 2022, https://www.cnbc.com/2022/04/04/walmart-saved-millions-from-elder-gift-card-scams.html.

51. Jennifer Strong, “How Retail is Using AI to Prevent Retail Fraud,” *MIT Technology Review*, September 20, 2022, https://www.technologyreview.com/2022/09/20/1059799/how-retail-is-using-ai-to-prevent-fraud/.

52. Dorota Owczarek, “eCommerce Fraud Prevention. Detect eCommerce Fraud With Machine Learning,” *Nexocode,* July 25, 2022, https://nexocode.com/blog/posts/ecommerce-fraud-prevention-and-detection-with-machine-learning/

53. Ibid.

54. Debby Gerbato, “What Grocers Need to Know About Gift Card Fraud,” Progressive Grocer, December 14, 2020, https://progressivegrocer.com/what-grocers-need-know-about-gift-card-fraud.

55. “Chip Technology Helps Reduce Counterfeit Fraud by 76 Percent,” *Visa* (blog), May 28, 2019, https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html.

56. “NFC: the Technology Behind Tap-and-Go Communication,” accessed October 12, 2022, https://clearbridgemobile.com/how-secure-are-nfc-mobile-payments/.

57. Vicki Hyman, “Swiping Left on Magnetic Stripes,” *Mastercard Newsroom* (blog), August 12, 2021, https://www.mastercard.com/news/perspectives/2021/magnetic-stripe/.

29. Shriya Roy, “Numberless Cards: No Visible Number or Code on Card Enhances User Security,” *Financialexpress*, July 26, 2020, https://www.financialexpress.com/industry/banking-finance/numberless-cards-no-visible-number-or-code-on-card-enhances-user-security/2034873/.

30. Jeremy Jojola, “Nearly 8,000 Card Numbers Stolen, 2 Arrested in Colorado in ‘skimming’ Case,” *KUSA*, March 22, 2022, https://www.9news.com/article/news/investigations/8000-card-numbers-stolen-skimming-colorado/73-bb63c27f-9c09-4f45-b41f-3029f6368939.

58. Shriya Roy, “Numberless Cards: No Visible Number or Code on Card Enhances User Security,” *Financialexpress*, July 26, 2020, https://www.financialexpress.com/industry/banking-finance/numberless-cards-no-visible-number-or-code-on-card-enhances-user-security/2034873/.

59. The FTC’s current “Stop Gift Card Scams” campaign and toolkit launched in December 2020. Reports of gift card fraud reported to the FTC in 2020 totaled $116 million. In 2021, consumers reported $223 million in losses related to gift card fraud. The FTC began tracking this data in 2017.

60. Chargeback Gurus, “EMV Chips & Liability Shift,” *Chargeback Gurus*, December 21, 2021, https://www.chargebackgurus.com/blog/emv-chips-liability-shift.

61. Mickael Gibrael, “EMV for Gas Stations - Stay Informed About the April 2021 Deadline,” Bankcard, March 25, 2021, https://www.getbankcard.com/blog/emv-for-gas-stations-april-2021-deadline-info/ and Chip Technology Helps Reduce Counterfeit Fraud by 76 Percent,” Visa, May 28, 2019, https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html.

62. Taylor Armerding, “Chip and PIN: No panacea, but worth the effort – and the cost,” *CSO Online,* September 22, 2014, https://www.csoonline.com/article/2685514/chip-and-pin-no-panacea-but-worth-the-effort-and-the-cost.html.

63. “How Much Does a Credit Card Cost to Make?”, last updated May 26, 2020, https://jleconsultants.com/how-much-does-a-credit-card-cost-to-make/.

64. Camille Desprez, “Uncovering the Real Cost of Digital Gift Cards,” *WeGift,* July 12, 2019, https://blog.wegift.io/uncovering-the-real-cost-of-digital-gift-cards.

65. Jeremy Jojola, “Nearly 8,000 Card Numbers Stolen, 2 Arrested in Colorado in ‘skimming’ Case,” KUSA, March 22, 2022, https://www.9news.com/article/news/investigations/8000-card-numbers-stolen-skimming-colorado/73-bb63c27f-9c09-4f45-b41f-3029f6368939.

66. Strong, “How Retail is Using AI to Prevent Retail Fraud,” https://www.technologyreview.com/2022/09/20/1059799/how-retail-is-using-ai-to-prevent-fraud/

ABOUT THE AUTHOR

Becca Trate is a policy analyst focusing on innovation in retail at ITIF's Center for Data Innovation. Previously, she worked as a communications manager for the National Association of Broadcasters. She holds a B.S. in Journalism from Ohio University.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation studies the intersection of data, technology, and public policy. With staff in Washington, London, and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the Information Technology and Innovation Foundation (ITIF), a nonprofit, nonpartisan think tank.

Contact: info@datainnovation.org

datainnovation.org