Working Collaboratively with Retailers to Fight Gift Card Fraud

Jilienne Gunther, MSW, JD
National Director of BankSafe, AARP

Debra Bailey Whitman, PhD
Chief Public Policy Officer, AARP
Introduction

Gift card sales have soared over the past few years and the trend shows no sign of slowing down, with market projections showing them to reach $221 billion by 2024.\(^1\) Unfortunately, soaring sales have been matched with an increase in gift card fraud. Gift cards are like cash, in that the convenience and ease of use they offer buyers also make them prime targets for perpetrators.

With gift card fraud, a scammer may pretend to be someone they are not in an attempt to convince the unsuspecting person to pay them in gift cards. This type of scam can take many forms:

- The scammer, claiming to be from “tech support,” says there is something wrong with a person’s computer, and that the person will need to pay in gift cards in order for tech support to fix the problem.
- Posing as a user of a dating site, the scammer says they have an emergency and need another site user to help them by buying them gift cards.
- Through a phone call the scammer pretends to be a relative in trouble who needs their target to send them gift cards.
- Claiming to be from the IRS or Social Security, the scammer states that the person has a fine or owes back taxes that can only be paid by gift card.
- The scammer impersonates the target’s utility company and threatens to shut off service unless they pay an overdue bill with gift cards.

Gift card fraud affects people of all ages, and the cost can be significant. By simply convincing a victim to provide the numbers on the back of a purchased gift card, perpetrators are able to quickly access and drain the funds, causing the average victim of gift card fraud to lose $1,000.\(^2\) Younger victims are twice as likely as older adults to lose money, but adults ages 70-79 lose about twice as much as adults ages 20-29 when they do get exploited. Worse, adults over the age of 80 lose four times as much as younger adults. Such impacts, regardless of age, become even more significant given that America is experiencing a savings crisis in which millions have no funds saved to cushion the blow.


This report offers a look at the gift card fraud issue from various angles before providing an assessment of industry’s role in intervention, both currently and in terms of future opportunities. This assessment is informed by a series of 1:1 interviews and surveys with more than 30 industry representatives as well as a comprehensive review of research and data from the Federal Trade Commission, non-profits, AARP and industry associations.

**FREQUENCY: GIFT CARD FRAUD HAS DOUBLED SINCE 2018**

Gift card fraud is among the payment methods scammers use most frequently. Unfortunately, its use has been on the rise during the pandemic, a time when people have been more vulnerable—financially, emotionally, and in other ways. Prior to the COVID-19 pandemic, the frequency of gift card fraud had actually been declining, with the number of instances reported in Q2 2020 being the lowest in two years. However, since the start of the pandemic, gift card fraud has rapidly increased, more than doubling in frequency. And of course, this doesn’t take into account those cases that are never reported.

The Federal Trade Commission’s (FTC) Consumer Sentinel Data Book, which ranks the 10 most frequently used payment methods in reported instances of scams, shows that gift cards rank in the top five in frequency (see Table 1). The only methods topping gift cards are credit cards (more than twice as likely as gift cards), debit cards, payment apps/services, and wire transfers.

**TABLE 1 - FREQUENCY OF FRAUD REPORTS BY PAYMENT METHOD 2020**

<table>
<thead>
<tr>
<th>Payment Type</th>
<th>Number of Fraud Reports</th>
<th>$ Amount Reported Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Cards</td>
<td>91,515</td>
<td>$149M</td>
</tr>
<tr>
<td>Debit Cards</td>
<td>63,352</td>
<td>$117M</td>
</tr>
<tr>
<td>Payment App or Service</td>
<td>61,903</td>
<td>$87M</td>
</tr>
<tr>
<td>Wire Transfer</td>
<td>56,811</td>
<td>$311M</td>
</tr>
<tr>
<td>Gift Card or Reload Card</td>
<td>43,242</td>
<td>$124M</td>
</tr>
<tr>
<td>Bank Transfer or Payment</td>
<td>17,039</td>
<td>$314M</td>
</tr>
<tr>
<td>Cash or Cash Advance</td>
<td>14,630</td>
<td>$146M</td>
</tr>
<tr>
<td>Cryptocurrency</td>
<td>11,710</td>
<td>$129M</td>
</tr>
<tr>
<td>Check</td>
<td>8,142</td>
<td>$87M</td>
</tr>
<tr>
<td>Money Order</td>
<td>3,872</td>
<td>$26M</td>
</tr>
</tbody>
</table>

IMPACT: FREQUENCY DRIVES EFFECT

Significant concern over gift card fraud stems from both the prevalence of gift cards—they are ubiquitous—and the fact that many victims may not be able to afford losing even a small amount of money. These may be some of the reasons why gift-card fraud attracts significantly more attention in the media and from non-profits than other forms of fraud.4

The greatest source of concern is how often gift cards are used as a form of payment. Gift cards are used 2.5-times more frequently than bank transfers/payments in fraudulent transactions involving scams. However, the amount a victim loses may be less than other forms of payments.5 It’s estimated that 2.5 times more money is lost from bank transfers or payments than from gift-card fraud (see Table 1).

Gift cards are used by countless retailers, making them a prime candidate for targeting from scammers. Perpetrators will often bounce from one payment method to another, as the industry works to make each method more secure. As the industry cracks down on bank transfers, perpetrators might switch to money orders. As security increases on money orders, they might switch to gift cards. And then the same thing happens even within a single payment method: as one major retailer tightens security on its own gift card, scammers are quick to change which cards they target.

Although losses may be lower on gift card fraud than other payment mechanisms, the impact on a victim is relative to the person’s resources. Today the nation is in the midst of a savings crisis. Roughly one in three US households say they would have difficulty paying a $400 emergency expense, highlighting the potentially debilitating impact of someone losing $1,000, the typical amount lost in gift card fraud.6,7

VICTIM AND SCAM PROFILE, AND PREVENTION CLUES

To understand how gift card fraud happens and how to prevent it, it is helpful to examine both the schemes used to manipulate a victim and the factors that make a person more vulnerable.

Common Schemes

Perpetrators have identified particularly successful schemes for convincing victims to purchase gift cards and, ultimately, turn over their money. Scammers demanding gift cards often start by impersonating a well-known business (32 percent) or government authority (20 percent), suggesting, for instance, the victim owes taxes or other back payment. By impersonating an authoritative entity, perpetrators apply pressure and seek to make victims fearful.

The FTC found that perpetrators most frequently initiate contact with their victims by phone (37 percent), a method that is more than twice as likely to be used than email (18 percent) and social media (16 percent), the two next most-frequent methods.9

Scammers often will stay on the phone with victims while they purchase the gift cards, coaching them on what to say in response to questions from a frontline employee. If the employee is successful in getting the victim to hang up, it is not uncommon for a victim’s phone to ring repeatedly to get them to reengage.

A scammer contacts a person with a phone call, email, text or social media message pretending to represent a company that the person may do business with, such as a bank or local power utility, or claims to be an IRS investigator. They use an urgent message—such as, “Your bill is overdue,” or, “You owe additional taxes”—to convince the person to make an immediate payment by wire transfer or gift card.

---

4 Miranda, “Scammers are tricking more people into buying gift cards.”
6 Federal Reserve Board Survey of Household Economics and Decision making (SHED).
8 Miranda, “Scammers are tricking more people into buying gift cards.”
9 Miranda, “Scammers are tricking more people into buying gift cards.”
Factors that Make Someone More Vulnerable

As with patterns that arise with the strategies scammer use, there are factors that make victims more susceptible. Though anyone can be the victim of a scam, AARP research\(^\text{10}\) has identified some specific environmental and emotional factors that were more common among fraud victims:

1. **Stressful life events.** At the time of a fraud incident, victims had experienced, or were experiencing, twice as many stressful life events—such as the death of a family member, loss of a job, or loneliness—compared to non-victims.

2. **Less family support, connection.** Fraud victims reported significantly less family support and closeness than non-victims.

3. **Stronger emotions.** Victims reported far stronger emotional responses during fraud encounters than non-victims who were able to spot a potentially fraudulent situation. These emotions were both positive (e.g., excitement when a scammer is promising cash, etc.) and negative (e.g., stress or fear) and led to more victims feeling out of control.

4. **Multiple Attempts.** On average, fraud victims reported 60 percent more fraud encounters than non-victims.

5. **Financial Stress.** AARP research also found that individuals facing financial strain are more likely to be vulnerable to scams. Those individuals are especially susceptible to scams that promise financial rewards or an opportunity to get out of debt.\(^\text{11}\)

In addition to financial circumstances, other behavioral factors have been found to play a large role in determining whether someone becomes the victim of fraud. In a joint report on victimization by the Financial Industry Regulatory Authority (FINRA), the Better Business Bureau, and Stanford University, researchers found that victimization by scams and fraud depends, in part, on **two-way engagement** between the target of the scam and the fraudster. Some individuals simply do not engage with a scammer; others engage but at some point recognize the deception and cease engagement. And finally, still others engage with the fraud and lose money (sometimes a lot of money).\(^\text{12}\)

The report found that 54 percent of respondents who were targeted and reported a scam had engaged with the perpetrator. While not all of those who engaged were victimized, those respondents who chose not to engage avoided the fraud altogether. This is significant given the environmental and emotional factors leading to scams—specifically the lack of social and family support.

The report also highlighted a key implication for combating fraud: *“More than half of people who reported a third-party intervention were able to avoid losing money.”*\(^\text{13}\) Following the previous examination of the scammer’s scheme and the victim’s state, this leads to the third piece of the equation, the one that provides the industry with an opportunity: behavioral intervention.

---


\(^{13}\) DeLiema, et al. “Exposed to Scams”
Behavioral Intervention: The BankSafe Link

The encouraging finding that third-party intervention can protect targeted individuals from becoming victims, is the reason AARP created the BankSafe training program, which trains frontline financial-institution staff to spot potentially fraudulent situations, particularly with older customers, before their money leaves their account. A random control study conducted by Virginia Tech examining the impact of AARP’s training found that when a frontline employee intervenes, they are able to stop fraud 50 percent of the time.

This experience shows the potential of training targeting retailers to accurately spot suspicious red flags and intervene in a dubious transaction as an effective approach to prevent gift card fraud.

ROLE OF THE INDUSTRY - MULTI-LEVEL EFFORTS TO STOP GIFT CARD FRAUD

With that base of experience and research showing the potential of third-party intervention to combat fraud, a similar strategy can be built around the key players in the gift card arena. To be sure, given the complexity and dynamics of how gift-card fraud works, stopping it will require the engagement of all key players.

Key Players

- **Consumers.** Because the perpetrator convinces the victim before a consumer even enters the store, it is critical to educate consumers on how to detect a scam and not engage.

- **Retailers.** With employees who engage directly with consumers, retailers are an important link in the gift card fraud prevention chain. Moreover, retailers can work closely with non-profits, gift card issuers, technology companies, industry regulators, and law enforcement, and become a hub for exploitation prevention.

- **Non-Profits.** Given the need for education and awareness, non-profit organizations can play a critical role, by providing information and tools for consumers and retailers and developing effective interventions at both levels. AARP’s BankSafe program and Fraud Prevention Network are good examples of this opportunity.

- **Industry Players.** Businesses and trade associations—for example, gift card packaging firms, gift card associations, and technology companies that create and develop retail point-of-sale (POS) systems—also can play a key role in advancing the tools and education used to stop exploitation.

- **Regulators and Law Enforcement.** Ultimately, industry regulators and law enforcement are a critical link in prosecuting perpetrators and setting industry expectations that allow for best practices in fraud protection to thrive.

These stakeholders agree that collaboration is key to reducing gift card fraud. Lisa LeBruno of the Retail Industry Leaders Association (RILA) stated, “There is no fail-safe way that retailers can guarantee that these types of scams will never occur using these products. However, more can be done by all stakeholders, including law enforcement, the companies that design, manufacture and service these reloadable pack cards, and merchants by providing consumer education, strengthening safeguards built into these products, and partnering with law enforcement to deter criminal activity on the front end, and arrest and prosecute criminals on the back end.”

In addition to the stakeholders LeBruno mentioned, non-profits, consumer advocates, and other groups also should do more to reduce gift card fraud by highlighting its evolving size and scope, increasing consumer awareness, and encouraging businesses to adopt effective interventions where reasonable.

14 Written Testimony of Lisa LaBruno Senior Vice President, Retail Industry Leaders Association (RILA) November 19, 2014.
Reputational Risk is a Key Motivator

While gift-card fraud may not be as high a priority as some other forms of loss prevention, most retailers report that a driving motivation for industry leaders to prevent this form of fraud is reputational risk and concerns about customer loyalty. As one mega-retailer stated, “We know there is a face behind the victim.” Customers will often blame the retailer for a loss (particularly when they don’t intervene) and will often seek a refund from the store. However, the store is often a third party in the transaction and has already reconciled payment with the card issuer making restitution difficult.

Retailers report that even though gift card fraud can be an infrequent event and isolated to one customer, awareness of that single fraud case can be multiplied when customers take to social media and complain about their experience.

Fraud prevention and consumer protection is often complicated by the fact that victims are in an elevated state of anxiety when the fraud is occurring and the store employees attempt to intervene. This leaves retailers with the challenge of trying to protect the consumer without providing what may be perceived as poor customer service.

The Next Achilles’ Heel: Mid-Size National Retailers

Many of the major retailers which have been frequently targeted for gift card fraud have made significant investments in preventing exploitation. But while that is a positive development, their vigilance may have unintended implications for other merchants.

Regulators charged with studying all consumer reports of fraud state that the top cards targeted for fraud have fluctuated over time from one major brand to another. The FTC reports that in the first nine months of 2021, the top gift card brands by amount lost were Target, Google Play, Apple, eBay and Walmart. Combined, those five brands represent more than half of the money lost to gift card fraud during that time ($84 million).\(^1\)

Yet as these companies’ make investments in prevention, there could be a negative impact on other companies. There is a concern that as these large companies become more effective and sophisticated in their fight against fraudsters, mid-sized retailers who haven’t made similar investments in training and technology may become the next target, if they have not already. Retailers and regulators have noted that “fraud is like a balloon,” in that when they push it out of one place, it shows up in another, as perpetrators will go wherever they can access the funds.

\(^1\) Miranda, “Scammers are tricking more people into buying gift cards.”
A LOOK AT INTERVENTIONS AND THEIR EFFECTIVENESS

Retailers have taken various steps to mitigate the risk of consumers falling prey to these scams, including employee training, customer and employee signage, point-of-sale enhancements, policies calling for staff to refuse a suspicious purchase of a gift card, technology improvements, and more. For example, many retailers train their staff to identify signs of common scams in order to prevent the transaction from proceeding and protect their customers from loss. In addition, many of these reloadable products have large labels directly on the package warning customers about the dangers of giving the PIN to unauthorized users. Point-of-sale displays can also be used to educate customers about the dangers of fraudsters.

On the technology side, the point-of-sale (POS) system can be an effective tool in combating gift card fraud. A POS system is a computerized network operated by a main computer and linked to several checkout terminals. POS technology enhancements have been integrated at the stores of the nation’s largest retailers to alert cashiers and the card vendor to possible suspicious activity and to stop a transaction when certain thresholds are met.16

Gift Card Fraud Frequency

While gift card fraud is clearly common, reliable data on frequency can be elusive, and so it is difficult to know exactly how often it occurs. Many victims do not report gift card fraud, particularly due to embarrassment of falling victim to a scam. Furthermore, given that the number of brick-and-mortar stores in total is in the hundreds of thousands, reported gift card fraud frequency per store location is very low (in absolute terms as well as relative to gift card sales) in many retail sectors. For example, one major retailer interviewed for this report sees “2.7 cases per day among their 2,000+ U.S. stores.” If these were evenly spread (which generally they are not) across that retailer’s stores, it would take more than two years for each store to see one instance, on average. A similar frequency was reported by another large retailer.

Furthermore, gift card fraud is not a top priority for retailers compared to other forms of loss prevention. Higher-priorities for retailers are shoplifting, hold-ups, and, more recently, labor shortages due to COVID-19. Thus, it is challenging to conduct research on gift card fraud in the retail location using a scientific random control trial, especially given the difficulty in administering such a trial in systematic fashion across an entire nation’s-worth of stores while weighting various factors. However, it is more plausible to measure the number of incidents reported before and after an intervention (e.g., staff training), especially when the retailer already has a central system to report incidents.

Store-Employee Training

Many mega-retailers conduct brief training sessions at least annually and sometimes quarterly. Retailers report that training is an effective and important form of prevention, but comes with challenges in implementation. As with any business decision, those challenges include cost relative to benefit. When considering whether to implement training, retailers must balance prevention with cost efficiency. Training represents non-revenue-producing activity and therefore “must be brief and to the point” as several mega-retailers pointed out. In addition, training also must be accessible and effective, as many cashiers tend to be younger without any previous on-the-job training on fraud prevention.

Despite the challenges, when done in an efficient and comprehensive manner, often with affirmative rewards or recognition, training can have an impressive impact on mitigating instances of gift card fraud. As one major national retailer with more than 9,000 retail locations in the U.S. put it, “We always see a spike in our employees flagging suspicious transactions for a month or two after training.” Such anecdotal evidence is confirmed by broader industry research, which finds that when cashiers do intervene, they are able to stop one out of every two instances of fraud, making them an important last line of defense.17 One big-box retailer said that after launching their mandatory training they have had an increase in the number of employees recognizing, stopping, and reporting gift card scams.

16 Written Testimony of Lisa LaBruno Senior Vice President, Retail Operations Retail Industry Leaders Association (RILA) November 19, 2014
17 DeLiema, et al. “Exposed to Scams”
The retailer reported that, “Our employees are seeing the fraud” and they want to know more about how to stop it while also maintaining the customer relationship.

It should be emphasized that to be effective, training must be repeated and updated. Perpetrators increasingly coach their targeted victims to avoid third-party intervention by providing specific scripts on how to respond to a retail employee’s questions. With perpetrators able to shift scripts and tactics at any time, frequently updated, interactive and regularly required training is more effective than static or infrequent training.

Empowering employees with the ability to take action is another key to a successful fraud protection program. It is critical that retailers adopt policies to allow frontline employees to decline a sale when they suspect a scam. Having a policy that allows store employees to refuse a suspicious transaction (as the industry reports that Walmart and CVS do) empowers them to put their training to the test. Given the success of cashiers stopping one out of two instances of gift card fraud when they speak up, these policies can be a game changer in reducing this kind of scam.

In-Store Consumer or Employee Signage

One prevention approach retailers have used is to display visible in-store awareness and warning signage related to gift card fraud. As it turns out, however, signage is challenging, and its effectiveness is questionable. Retailers explain that “shelf and display space is at a premium due to highly valuable product placement.” And while some retailers implement gift card warnings, they nevertheless report the tool is for the most part ineffective. Multiple retailers point out that because the victims are often in a fear bubble when they set foot in the store, and they are convinced of the perpetrators’ authenticity, customers are quick to dismiss warnings on signage and packaging, as they simply don’t believe they’re falling for a scam.

Employee posters in break rooms may be an option, although, “It’s a hard sell to get our retail locations to properly install all displays we provide them,” as a retailer with over 2,000 locations reports. Some also pointed out that many locations do not maintain or replace ripped or damaged signage. And many customers and staff may not read these messages.

Technology Innovations in Point-of-Sale Systems

Larger retailers typically have POS systems that trigger alerts to the cashier that fraud may be in the process of happening. Triggers include gift card purchases over a specified dollar amount as well as the number of cards (e.g., 5) purchased at once.

In some cases, cashiers are given an on-screen prompt to ask a question about potential gift card fraud. Some retailers arm cashiers with gift card warning sheets that they can give customers as a means of intervening. In the most sophisticated retail environments, cameras (trained on the POS station with the suspicious purchase) alert fraud risk-managers who can zoom in and connect with the store.

These systems can be extremely effective, but, again, their reach is limited to only larger retailers who can afford the high cost to install and maintain them. Moreover, there are still many retailers who aren’t the frequent targets of gift card fraud and do not utilize these systems (e.g., fast casual restaurants, specialty clothing stores, etc.). And smaller retailers of course are far less likely to have POS systems, providing an enticement for fraudsters to move downstream to these more vulnerable businesses.
The most common POS interventions are listed below:

**Monitoring / Alerts / Restrictions**

- Alerts to odd or suspicious purchases triggered by purchase amounts and number of gift cards being purchased at one time.
- Monitoring large third-party gift card purchases by store to see if a store is more susceptible to fraud than other locations.
- Effective monitoring of gift card balance inquiries to detect bots and hack attacks.
- Limiting the quantity of certain products consumers can purchase at one time.
- Delayed redemption on money card loads to allow gift card processors to investigate.
- Sending bulk purchases through corporate offices rather than in the retail store.
- Store-manager approval needed for high dollar in-store purchases.
- Preventing purchasing of gift cards with other gift cards (AML, or anti-money laundering, protection).
- Limiting gift card purchases on the same credit card within a three-day period.

**Pin Requirements**

- Requiring the card’s PIN for balance inquiry. Evaluating effective gift card sequences and PINs to avoid back-end hacks.
- Not allowing employees to hand key the gift card number without a PIN.
- Requiring the gift card PIN for purchases.
CONCLUSIONS AND RECOMMENDATIONS

Americans reported losing $124 million due to gift card fraud in 2020 with the average victim losing $1,000. As this payment form remains popular among consumers, action must be taken to prevent these frequent, persistent losses. Three keys to successfully addressing the problem have emerged: consumer education, employee training, and POS enhancements.

Consumer Education

The more educated consumers can become about gift card scams, the more likely they will be able to elude engagement with perpetrators and avoid the problem before it even gets started. Tools like AARP Fraud Watch Network’s Gift Card Payment Scams and the FTC’s Gift Card Scams are a terrific start when it comes to consumer education. Alerting the media to the issue and helping to generate media stories of gift-card victimization are another effective way to both increase awareness of these scams and normalize the issue for victims who may be too embarrassed to come forward.

The goals of increased consumer education should be three-fold. First, education efforts should grow the percentage of consumers, currently 47 percent, who choose not to engage with a perpetrator when they are contacted. Second, consumer education must increase the likelihood that, should a consumer engage with a perpetrator, they will identify the scam before even attempting to purchase gift cards. Finally, should a consumer be convinced the perpetrator is legitimate, education efforts must increase the likelihood that consumers will be more likely to listen to a friend, family member, or retail employee when they intervene.

Employee Training and Policy Allowing Refusal of Suspicious Gift Card Transactions

Consumer education alone will not solve the problem. Retailers could provide a critical safety net to consumers who are attempting to purchase gift cards in fraudulent situations. The two most powerful tools for a retail employee to keep a consumer from being scammed are knowing (1) what behaviors to be on the lookout for (e.g., buying multiple cards of the same brand, being on the phone throughout the attempted transaction, seeming anxious or agitated) and (2) what to say to the consumer when they see red flags of gift card fraud.

With about half of all instances of exploitation being stopped when an employee intervenes, arming employees with the knowledge, skills, and confidence to spot red flags and then effectively intervene will allow retailers to stop more instances of fraud. AARP BankSafe has invested resources in developing a free employee training platform for retailers. This interactive online training provides frontline employees with the confidence and skills to stop the suspicious transaction.

In conjunction with employee training, putting in place a policy that allows employees to refuse a suspicious gift card purchase is critical.

POS Enhancements

As mega-retailers who have invested in the technology know, artificial intelligence-based POS enhancements and other tech tools that alert employees to suspicious transactions are highly effective. Not only do such tools provide a prompt for an employee to recall their education and training, they also show a level of corporate concern that the employee can point to as they engage with the potential victim, thus allowing the situation to illustrate customer care—and not poor customer service.

Through the powerful combination of consumer education, employee training, and POS enhancements, gift card fraud can be dramatically reduced. This will help protect the financial well-being of countless potential victims, including older adults, who often are most vulnerable to both scams and the potential financial impact.
Acknowledgments

This paper is made possible thanks to research conducted by the Defined Contribution Institutional Investment Association in collaboration with representatives from major US retailers, card issuers and industry associations. We are grateful to our colleagues at AARP—Gary Koenig, and Susan C. Reinhard—for their continual support and edits. We look forward to continued collaboration with key partners to fight gift card fraud and stop financial exploitation.