

# GIFT CARDS AND SCAM PAYMENTS: PROTECT YOUR CUSTOMERS

Gift card scams continue to be a significant risk for consumers. While financial institutions don't directly handle gift card transactions, educating customers about gift card scams helps protect them from fraud and can strengthen trust. In many scam scenarios, criminals instruct victims to make payments using retail gift cards. Gift cards are familiar to most people, widely available for purchase and difficult to trace. The funds also are accessible immediately. These scams typically involve high-pressure impersonation tactics, with the criminal claiming to be from a familiar organization to trick victims into buying cards and sharing the personal identification number (PIN). Once the card information is obtained, criminals quickly drain the funds and disappear.



## WHY CRIMINALS PREFER GIFT CARDS

- **Immediate access:** Funds are available instantly once card details are obtained
- **Limited traceability:** More difficult to track than traditional payment methods
- **Widespread availability:** Easy to purchase at numerous retail locations
- **Low security:** Circumvents payments fraud detection methods that are based on customer profiles and account activity

## IMPOSTOR SCAMS AND GIFT CARDS

Criminals use various impersonation strategies and will take desperate measures to execute scams. In each scenario, criminals demand payment using retail gift cards.

Impostor Type	Family Members/Friends	Government Agencies	Lottery/Prize Winners
Scam Strategy	Urgently requesting money for an emergency. Often use artificial intelligence (AI) voice cloning to make the scheme seem even more realistic	Demanding payment for delinquent taxes or to maintain benefits	Won a prize/lottery but requesting money to help pay taxes in advance via gift cards

# GIFT CARDS AND SCAM PAYMENTS: PROTECT YOUR CUSTOMERS

Below are two examples of gift card scams impacting individuals and businesses.



## EXAMPLE 1: IMPOSTOR SCAM TARGETING INDIVIDUALS

Criminals pose as representatives of utility companies, such as electric or cable TV providers. They contact individuals via phone calls and text messages with urgent notices that service will be shut off due to a missed payment. The scam relies on creating a sense of urgency – victims often panic at the threat of losing essential services and act without verifying the claim. Criminals instruct individuals to purchase gift cards, claiming this is the only way to avoid disconnection. Victims then are told to provide gift card numbers and PINs or send photos of the cards. Once criminals obtain this information, they quickly use the gift card funds to purchase goods they can sell or they transfer the value to accounts they control. The scam victims lose the amount of the gift cards and may not be able to recover the value.

## EXAMPLE 2: IMPOSTOR SCAM TARGETING BUSINESSES

Criminals impersonate company executives who instruct employees planning an upcoming gathering to purchase gift cards as a token of appreciation for all associates. The requests typically appear to come from actual executives or managers, but the phone numbers or email addresses are spoofed – manipulated to appear to be from a trusted source.

Criminals create urgency and pressure employees to act immediately, leaving little time to verify the request or discover the scam. They impose fake deadlines and ask employees to provide the gift card numbers and PINs as soon as possible. Once criminals obtain the gift card information, they quickly drain the funds or sell the cards online at a discounted rate. By the time the employees realize the request was fraudulent, the gift cards are worthless, and the funds likely are unrecoverable. In this scenario, businesses take the loss for the total amounts spent to purchase the gift cards.



# GIFT CARDS AND SCAM PAYMENTS: PROTECT YOUR CUSTOMERS

## INCREASE CUSTOMER AWARENESS OF GIFT CARD SCAMS

Financial institutions can help educate their customers about gift card scams:

If someone demands payment with a retail gift card, it could be a scam. **Legitimate organizations rarely accept retail gift cards as payment for services, fines or taxes.** While prepaid debit cards are legitimate payment methods used by some individuals, criminals often request gift cards because of their immediate funds availability and limited traceability.

### Encourage Customers to Watch for These Red Flags



- Urgent demands for immediate payment
- Threats of arrest, legal action or loss of service
- Requests to keep the transaction secret
- Instructions to read gift card numbers over the phone or send photos of cards

### Financial Institution Safeguards



- Train staff to recognize unusual cash withdrawals that may indicate a scam in progress
- Implement monitoring systems for unusual purchases of gift cards using bank-issued cards
- Create educational resources highlighting common scam scenarios that involve gift card payments
- Establish clear protocols for assisting scam victims

### When Customers Fall Victim

If a customer has been scammed through gift cards:



1. Advise them to contact the gift card company immediately to report the fraud
2. If purchased using a debit or credit card, recommend they notify their card issuer
3. Encourage reporting to the Federal Trade Commission (FTC) at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)
4. Be sensitive to the situation and provide reassurance to help the customer cope with the impact

## CONCLUSION: AVOID SCAMS THAT DEMAND PAYMENT BY GIFT CARD

Gift card payment demands are often warning signs of a scam. By educating customers about this risk, financial institutions help protect their customers' financial security while strengthening institutional trust and relationships.

*The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, use of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.*