Card Tricks: The Evolution of Medicare Card Scams is More Than Magic

Jennifer Trussell
Fraud Prevention Consultant

Medicare card scams have been a consistent fraud trend for decades. They have evolved from people offering "$50 for a copy of your red, white, and blue card" to robocallers telling beneficiaries their Medicare benefits might be shut off if they do not accept a new card. This article gives an overview of the most common Medicare card schemes, along with the opportunistic methods that scammers use to convince beneficiaries to provide their number. Many of the tactics never get old, as they reappear in cycles over time.

Favorite Card Tricks

When Medicare cards contained Social Security numbers (SSNs) prior to 2018, the primary lure for scammers was to obtain a copy of the card so they could steal the beneficiary's SSN and/or obtain medical benefits under a stolen identity. An old card trick was to simply offer a beneficiary a particular sum of money to copy their card. The card number (an SSN with a letter suffix) was then used along with other personally identifiable information (PII), such as name and date of birth (DOB), to obtain medical benefits under a false identity. Since many health care providers required a copy of the card as insurance proof for their paper files, a copy of the card was more valuable than just the number. However, the SSN and PII were still of interest to the scammer for other types of medical identity theft, especially benefits fraud. With the advent of electronic health care billing, the number and suffix became more valuable as scammers began to bill Medicare for services not rendered on multiple occasions for multiple beneficiaries, as opposed to just using the card to obtain individual medical care under false pretenses.

The COVID-19 pandemic provided an opportunity for scammers to prey on socially isolated beneficiaries willing to pick up the phone.

Although scammers would continue to hound beneficiaries by phone, in person, and eventually through email and social media for their Medicare numbers, the issuance of new cards in 2018 to 2019 by the Centers for Medicare & Medicaid Services (CMS) resulted in a new variety of excuses used by scammers. Many of them centered around the type of card and included:

- You need a new laminated card.

- You need a new plastic card.
- You need a new plastic card with a security chip.
- Medicare cards are changing colors this year. You need a new (name the color) card.
- You need a new silver or gold card (to imply a certain status like rewards benefits or airline miles).

The COVID-19 pandemic provided an opportunity for scammers to prey on socially isolated beneficiaries willing to pick up the phone. New card scams during this period included:

- Medicare is requiring you to get a new Medicare card due to COVID.
- Your current card does not cover COVID care, so we need to issue you a new card.
- Your medical history indicates you may be at risk for COVID complications, so we need to issue you a special Medicare card.

Once the word got out that beneficiaries didn't need a new type of card, or a new card to receive COVID services, the card tricksters began to use other tactics, including:

- It's a new year so you need a new card.
- Your card is expiring so we need to send you a new one.
- Your Medicare status needs to be updated, and we'll then update it on a new card.

The Mind-reading Card Trick

As discussed in the article Be on the Lookout (BOLO) for Social Engineering Schemes in the March 2023 edition of *Medicare Messenger*, scammers have begun using increasingly sophisticated methods to convince Medicare beneficiaries they are legitimately from Medicare and that a new card is required. Experienced criminals are often good at picking up on verbal or written response cues and almost seem to "read the mind" of the beneficiary. In the social engineering cycle of investigation, hook, play, and exit, the hook portion of the cycle becomes extremely important as the scammer establishes rapport with the victim, convinces them of the legitimacy of the call/caller, and takes control of the conversation. Sometimes this is accomplished by positive language (appealing to the victim's curiosity or offering free services) or reward offers such as:

Experienced criminals are often good at picking up on verbal or written response cues and almost seem to "read the mind" of the beneficiary.

- You may be eligible for additional benefits (e.g., dental, vision) so we need to review your eligibility and issue you a new card.
- Do you have a family history of cancer? If so, we need to issue you a new Medicare card that covers cancer care.

Experienced scammers may also use a neutral hook, requiring a

response such as:

- Have you received your new Medicare card? Since you haven't, what is your number so I can verify it was sent?
- You may have received the wrong Medicare card. Let's verify your number to ensure you've been issued the correct card.
- You've been issued a new Medicare card. What is your Medicare number so we can activate your new card?
- Medicare is issuing new cards, and we need to verify the current date of birth, address, and Medicare number we have on file.

Of concern, some scammers are using aggressive scare tactics, especially with vulnerable beneficiaries. These tactics include:

- If you are not issued a new card, your Medicare benefits may be terminated.
- Due to your medical conditions, you are at high risk for COVID. You need to answer a few questions (or participate in a telemedicine visit) or Medicare will not pay for your care related to COVID. Once you answer these questions, you'll be issued a new Medicare card.
- There has been suspicious activity on your Medicare account. You need to verify your Medicare number and answer a few questions so we can unlock your account.
- Do not question me. You need to be issued a new Medicare card.
- You need to pay a fee to get a new Medicare card with a security chip. What is your Medicare number and what credit card would you like to use?

Of concern, some scammers are using aggressive scare tactics, especially with vulnerable beneficiaries.

Turn the Tables on the Scammers

There seems to be no end to the variety of tactics the scammers use to obtain the Medicare number of unsuspecting beneficiaries. The latest scheme involves prepaid debit cards, known as Medicare flex cards, available through some Medicare Advantage (MA) plans. Scammers impersonate an MA plan representative to obtain their Medicare number under the pretense of issuing a special deal on a flex card. What's a beneficiary to do? Turning the tables on the scammers by preventing fraud from happening in the first place is always the best move. The SMP Resource Center has updated its Medicare Card Scams page in the Fraud Schemes section of its public website. Resources include additional Medicare card scams information, a tip sheet, and infographics. Be your own magician and be on the lookout for Medicare card scams.

This project was supported, in part, by grant numbers 90SATC0002 and 90MPRC0002 from the U.S. Administration for Community Living, Department of Health and Human Services, Washington, D.C. 20201. Grantees undertaking projects under government sponsorship are encouraged to express freely their findings and conclusions. Points of view or opinions do not, therefore, necessarily represent official Administration for Community Living policy.