Health Care Scams and Consumer Protection

Presenter: Tracey Thomas
Federal Trade Commission, Bureau of Consumer Protection, Division of Marketing Practices
January 28, 2016

The views expressed are those of the speaker and do not necessarily represent the views of the Federal Trade Commission or any other person.
Health Care Scams and Consumer Protection

Topics of Discussion

• (Very) Quick overview of ACA Marketplaces
• Common Health Care Scams and FTC Cases
• Tips on Presenting Information to Beneficiaries
• Resources for Advocates
  • Pass It On
  • Identity Theft Resources
• Telemarketing Sales Rule Amendments
The Affordable Care Act (ACA)

(Very) Quick Overview of Marketplaces

• Health Insurance Marketplace and the (ACA)
  • Provides health insurance, with a choice of plans and levels of coverage
  • Consumers may be eligible for tax credits to lower the premiums or reduced cost sharing to lower out-of-pocket spending
  • States can choose to run their own marketplace, partner with the federal govn’t, or have the federal govn’t run their exchange (consumers can get to all marketplaces through healthcare.gov)
  • Marketplace open enrollment period last year was November 1 - December 15, 2015
• New insurance available through the marketplaces **does not** affect Medicare eligibility of seniors

• Medicare’s most recent open enrollment period was October 15 - December 7, 2015
New programs make headlines

Consumers may have some (but not all) information about the ACA

General concerns about how new programs will affect them
Common Health Care Scams

- Medicare Scams/Government Imposters
- Medical Discount Plans
Medicare Scams

• Typical form of scam is government imposter
• Telemarketers pose as Medicare or another government agency to convince consumers to provide sensitive information
• Callers often prey on seniors’ fear of losing Medicare
• Those seniors not yet eligible for Medicare may also be vulnerable to fraudsters’ promises of cheaper/better insurance
• Potential for ID theft and loss of money (through theft directly from bank accounts, sham services, etc.)
• Medicare/Government Imposter Scam
• The Pitch:
  • FTC alleged that defendants called consumers and pretended to be affiliated with Medicare
  • Telemarketers claimed that they were providing consumers new Medicare cards and needed to “verify” their information
  • Requested bank account number as verification
  • Implied that consumers could lose benefits if they didn’t comply
  • Used the information to take money from consumers’ bank accounts without their consent
FTC v Sun Bright Ventures

• The Reality
  • Defendants used the information to take money from consumers’ bank accounts without their consent
  • Typical debit was $399
• Consumers looking for healthcare are contacted by company that appears to offer legitimate, full-coverage health insurance for a low price
• Usually many attractive claims (widely accepted, qualified health plan/endorsed by govn’t, consumer eligible despite age or pre-existing conditions, etc.)
Medical Discount Plans

• The Reality:
  • The product is actually a discount club membership that is NOT health insurance and often provides no real discounts or coverage
  • Identity thieves also use pitches for medical discount plans and insurance to get your personal information.
• Medical Discount Plan Scam
• The Pitch
  • Defendants lured consumers in with promises of cheaper health insurance
  • Claimed it was a traditional health plan that was widely accepted
  • Used health care “lingo” (”co-pay,” “deductible,” “pre-existing condition”)
  • Claimed to be a non-profit
  • Claimed offer was available for a limited time
  • Cost included one-time enrollment fee of $50 to several hundred dollars. Also monthly fee ranging from $40 to $1000.
The Reality

- Consumers bought a membership that supposedly offered discounts on various products services, including some health services.
- Consumers discovered they couldn’t actually use the plan for much of anything, especially health-related costs.
QUESTIONS...?
FTC Resources for Advocates

- Consumer education for active older adults – [www.ftc.gov/passiton](http://www.ftc.gov/passiton)
- Respecting a lifetime of experience
- Encouraging information sharing on:
  - identity theft
  - imposter scams
  - charity fraud
  - health care scams
  - paying too much
  - “you’ve won” scams
Pass It On Overall Message:
- “You’ve got this. But you probably know someone who doesn’t. So pass it on. Share what you know.”
- Not more vulnerable
- Not a frail victim
- Part of the solution, not the problem
Presenting Information to Constituents

Health Care Scams

They say you need...

- A new Medicare card
- A new health insurance card
- Discounted health insurance
- To act now!
Presenting Information to Constituents

Health Care Scams

But you don’t need...

• To get a new Medicare or insurance card
• To buy bogus discounted insurance
• To act now
Presenting Information to Constituents

The real story

- Scammers want your:
  - Social Security number
  - Financial information
  - Insurance number
  - Money
Identitytheft.gov

- Federal government’s one-stop resource to help you report and recover from identity theft.
- Created for people who have been victims of identity theft.
- **New feature:** personalized recovery plan for individual consumers
  - tailored recovery plans for more than 30 different types of identity theft
- Provides detailed advice, such as:
  - Getting a credit report
  - Getting an Identity Theft Affidavit
  - Getting a police report
  - easy-to-print checklists, and
  - sample letters
QUESTIONS...?
1. Prohibits certain “*abusive*” practices, such as:

- The use of threats, intimidation, profanity
- Requesting or receiving *advanced fees* for:
  - credit repair services
  - recovery services
  - obtaining a loan or other extension of credit
  - debt relief services
- Causing billing information to be submitted for payment, directly or indirectly, without the *express informed consent* of the customer
- Initiating outbound calls to telephone numbers on the Do Not Call Registry
- Abandoning outbound telephone calls
- Engaging in most pre-recorded telephone calls
2. Prohibits “deceptive” telemarketing acts or practices, such as:

- Failing to affirmatively disclose key information (likely to affect the consumer’s decision to purchase) *before* a customer pays.
- Making material misrepresentations of key information.
- Causing billing information to be submitted without the *express verifiable authorization* of consumer for certain payment methods, including credit/debit cards, ACH, EFTs).
- Making material misrepresentations in connection with the solicitation of a charitable contribution.
3. Prohibits:
   - Providing *substantial assistance* to a seller or telemarketer when the person *knows or consciously avoids knowing* that the seller or telemarketer is violating provisions of the Rule:
     • Lead Generators and Data Brokers
     • Fulfilment Houses
     • Voiceblasters
     • Payments Participants; and
     • Credit card laundering or “factoring.”
Actions against telemarketers and sellers engaged in deceptive or abusive conduct, while marketing a variety of products and services:

- Medical discount cards/Medicare/Medical alert devices
- Credit card interest rate reduction services
- Business coaching/business opportunities
- Government grants
- Payday loans
- Mortgage/foreclosure/debt relief services
1. **Anti-Fraud Amendments**
   - Novel Payment Methods
   - Recovery Services

2. **Clarifying/Miscellaneous Amendments**
   - Do Not Call Provisions
   - Express Verifiable Authorization
   - Business to Business Exemption
Novel Payment Methods

Prohibit the use of the following payment methods in all telemarketing transactions:

- Remotely Created Payment Orders ("RCPOs"), including Remotely Created Checks ("RCCs")
- Cash-to-Cash Money Transfers
- Cash Reload Mechanisms
Remotely created payment order (RCPO) means any payment instruction or order drawn on a person’s account that is created by the payee or the payee’s agent and deposited into or cleared through the check clearing system.

Example: Remotely created checks (RCCs)
Cash-to-cash money transfer means the electronic transfer of the value of cash received from one person to another person in a different location that is sent by a money transfer provider and received in the form of cash.

Examples: Western Union, Moneygram
Cash reload mechanism means a device, authorization code, personal identification number, or other security measure that makes it possible for a person to convert cash into an electronic form that can be used to add funds to a general-use prepaid card, or an account with a payment intermediary.

Examples: MoneyPak (discontinued) or REloadit
Clarifying Amendments (FYI)

- 310.4(b) - Clarify that calls to a person listed on the Registry are permitted only if the seller or telemarketer can demonstrate existence of express written agreement (“EWA”) or existing business relationship (“EBR”).
- 310.4(b)(1)(ii) - Expressly state examples of the types of impermissible burdens on consumers that constitute “denying or interfering with” their right to be placed on an entity-specific do-not-call list.
- 310.3(a)(3)(ii) - Clarify that audio-recorded express verifiable authorizations (“EVA”) must include an accurate description of the goods or services.
- 310.6(b)(7) - Clarify that the B2B exemption extends only to calls inducing a sale or contribution from the business, and not to calls inducing sales or contributions from individuals employed by the business.
- 310.8(c) - Tighten the prohibition against sellers sharing the cost of DNC Registry fees to close an enforcement loophole.

- Effective date: June 13, 2016 (anti-fraud amendments).
- Effective date: February 12, 2016 (all other amendments).
Referring Cases to the FTC

- Consumer Sentinel Database
  - National database of consumer fraud, identity theft, and Do-Not-Call complaints maintained by the FTC
  - Available to over 2100 federal, state, and international law enforcement agencies
- Include as much information as possible (names of telemarketers or business owners, phone numbers, websites, dates of communications, etc)
- The person filing a complaint does not have to be the victim of a crime—you can report practices or companies you think are behaving unfairly or deceptively.
- Keep in mind: No individual resolution of complaints
- To file complaints directly with the FTC:
  - Online: Ftc.gov/complaint
  - By Phone: 877-FTC-HELP (877-382-4357)
QUESTIONS OR COMMENTS?

Tracey Thomas
tthomas@ftc.gov
202-326-2704