South Carolina
DEPARTMENT OF CONSUMER AFFAIRS
293 Greystone Boulevard Suite 400
P. O. BOX 5757
COLUMBIA, SC 29250-5757

Carri Grube Lybarker
Administrator/
Consumer Advocate

PROTECTING CONSUMERS SINCE 1975

January 24, 2022

Via Electronic Submission
Faye I. Lipsky, Federal Register Liaison
Office of Regulations and Reports Clearance
Social Security Administration
3100 West High Rise Building, 6401 Security Boulevard
Baltimore, Maryland 21235-6401

RE: Docket No. SSA-2021-0006
Addressing Certain Types of Fraud Affecting Medicare Income Related Monthly Adjusted Amounts (IRMAA)

Dear Ms. Lipsky:

The South Carolina Department of Consumer Affairs ("SCDCA"/"Department") is pleased to offer comments in response to the Social Security Administration's ("Administration") advance notice of proposed rulemaking ("ANPRM") to address certain types of fraud affecting Medicare income related monthly adjusted amounts ("IRMAA").

Established in 1974, SCDCA is South Carolina's consumer protection agency. SCDCA helps formulate and modify consumer laws, policies, and regulations; resolves complaints arising out of the production, promotion, or sale of consumer goods or services in South Carolina, whether or not credit is involved; and promotes a healthy competitive business climate with mutual confidence between buyers and sellers. SCDCA is responsible for the administration and enforcement of over 120 state and federal laws. A large part of our authority stems from Title 37 of the South Carolina Code of Laws, the Consumer Protection Code, of which the Financial Identity Fraud and Identity Theft Protection Act[1] is a part. Overall, SCDCA protects consumers while giving due regard to those businesses acting in a fair and honest manner.

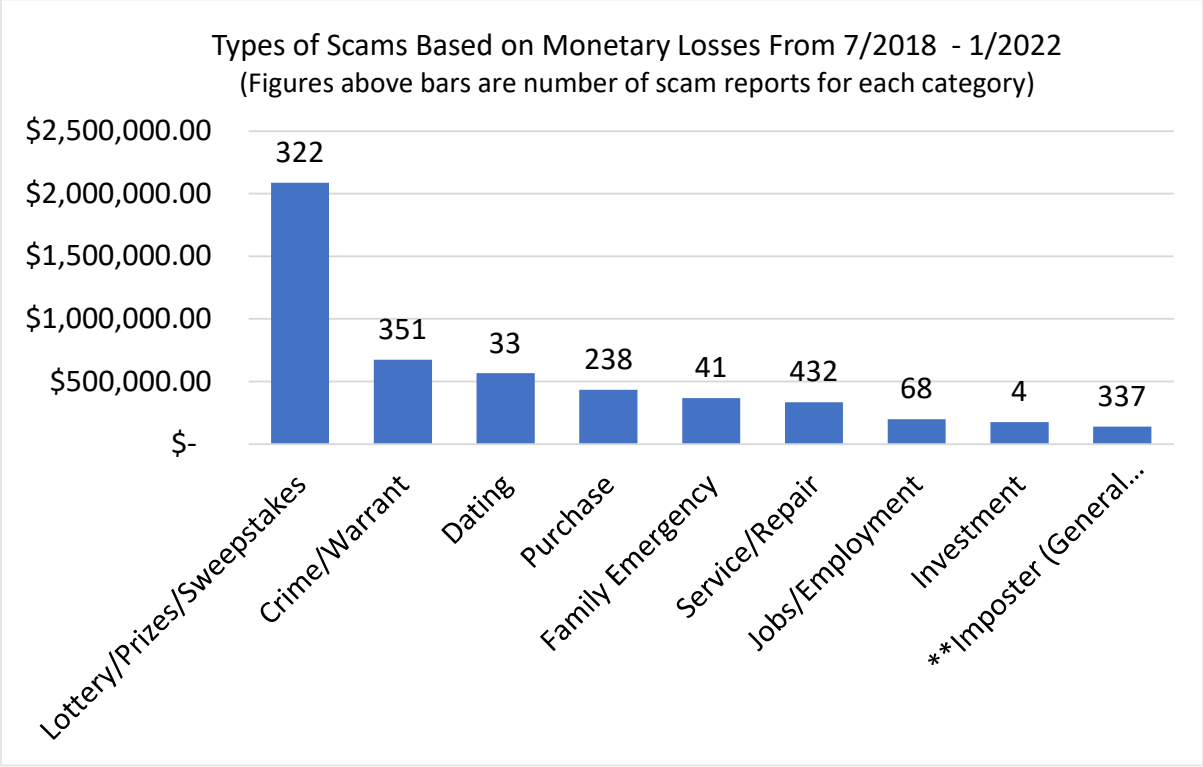
[1] *S.C. Code Ann.* § 37-20-110 *et seq.*, Consumer Identity Theft Protection.

In 2012, the South Carolina General Assembly funded the Identity Theft Unit ("IDTU"), one of the Divisions of the Department. The IDTU provides guidance and outreach in the form of postings, presentations, and publications to consumers to prevent identity theft and assist those who are identity theft victims. The IDTU also receives consumer scam reports and provides guidance and information to scam victims. By tracking scams and educating consumers, the IDTU mitigates the harms caused by scammers.

The Administration has requested input from the public to more fully understand the forms of fraudulent activity affecting beneficiaries and to determine how the Administration might revise its rules to better assist victim-beneficiaries. SCDCA supports the Administration's efforts to provide relief to beneficiaries affected by fraud and offers the following comments regarding scams affecting South Carolina consumers, potential forms of evidence, and balancing evidentiary needs and requirements. These comments are based upon SCDCA's experience in administering and enforcing identity theft protection statutes, processing consumer complaints and scam reports, and otherwise assisting South Carolina consumers when their personal information or money is stolen.

Types of Scams and Contact Methods in South Carolina

The IDTU received 3,309 scam reports between July 2018 and January 2022. The Department categorizes scam reports, and includes some of the top categories by monetary losses in the chart below.



The following are descriptions of the types of scams:

Lottery/Prizes/Sweepstakes - Consumer gets a call, email, mail, telling them that they have won a lottery, sweepstakes, or other prize, but needs to first pay a fee (for taxes, custom fees, etc.) to collect their winnings. Examples: Publishers Clearinghouse; foreign lottery. South Carolina consumers have lost over $2M.

Crime/Warrant – Scammers claim a warrant or citation has been issued in a consumer's name for crimes/offenses that they did not commit. Example: A warrant is out for your arrest because your social security card was found at a scene of a crime. South Carolina consumers have lost over $674,124.

Purchase - Consumer directed to or approached by imposter business to trick consumer into paying for fake consumer goods. Most online purchase scams occur when a payment is made online to purchase something, and nothing is delivered. For example, a consumer exchanges money for a vehicle with a scammer, and the vehicle is never delivered, or the scammer drops contact. South Carolina consumers have lost over $430,000.

Dating - Scammers usually establish fake dating profiles with the intention of extorting money. The fraudsters pretend to be someone out of the country on a religious mission, military deployment or business. Example: A consumer entrusts a scammer she met for dating who then asks for money to pay travel expenses, medical bills or other costs. South Carolina consumers have lost over $565,000.

Family Emergency - Scammer claims a friend or relative is in an emergency and needs money. Example: Scammer claims to be a public defender and claims a consumer's grandson is in jail and needs cash mailed to post bail. South Carolina consumers have lost over $365,000.

Jobs/Employment - Consumer is often offered a job by a "hiring manager" without having an interview; after being "hired," the scammer will tell the consumer that they must pay upfront for training/certification; scammer may also ask consumer for PII and banking information in or to run a credit check and/or set up direct deposit. Example: Consumer receives an email regarding a job opportunity and purchases $20K in supplies and equipment, and then received reimbursement payments that are all insufficient funds. South Carolina consumers have lost almost $200,000.

Service/Repair - Consumer is directed to or approached by imposter business to trick consumer into paying for a fake service or repair. Example: A consumer has a pop-up on their computer that says the computer is infected with a virus and must contact technical support to fix the issue. The consumer calls the number displayed and is convinced to pay the scammer to have the virus removed. South Carolina consumers have lost almost $335,000.

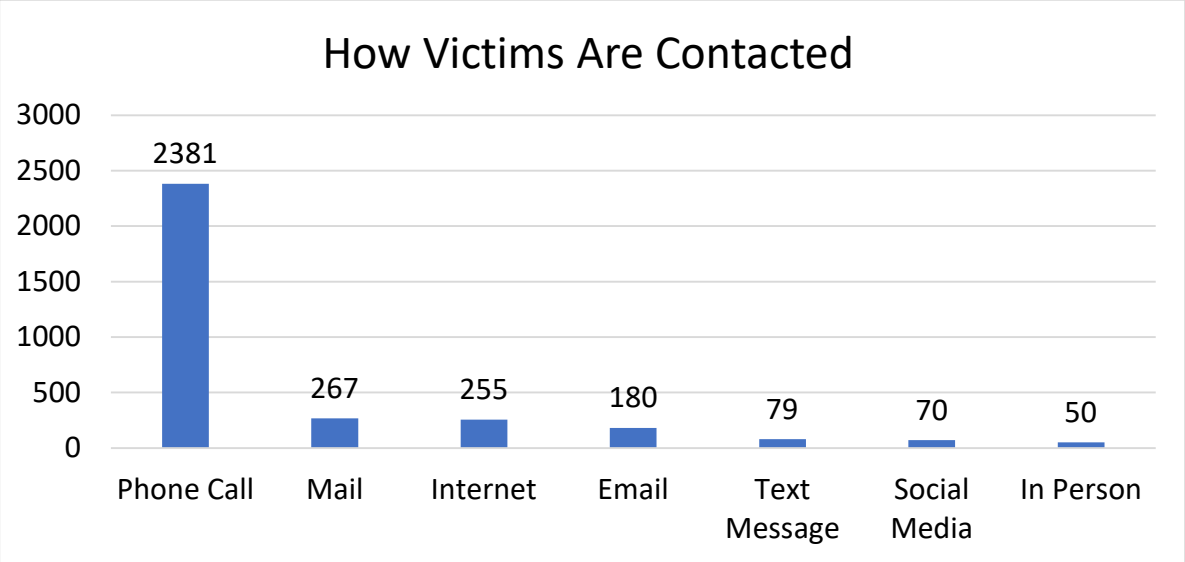
Investment - Investment opportunities in day trading, gold, art, coins, scam companies that offer advice or seminars on investment. Example: A consumer finds information on a company

claiming to be a gold investment group on the internet. The consumer sends funds in exchange for gold but never receives the gold. South Carolina consumers have lost over $175,000.

Imposter (General Business) - Someone pretends to be a trusted person/organization to get consumers to send money or give personal information. South Carolina consumers have lost over $138,000. **The chart reflects data up to June 2019 for this type of scam. After this time, we updated our category descriptions and these scam types now fall under various other categories.

These reports indicate consumers paid fraudsters and scammers over $5.5M during this time; however, this figure does not include certain tailing consequences greater.[2] Also, based on the Department's outreach experience, we know not all consumers file reports of scams with our office, and therefore, the number of scams and corresponding losses incurred are likely even higher.

As shown in the chart below, phone calls are the most utilized means of contacting consumers according to our scam report data. In the lottery, prize or sweepstake category, phone calls accounted for over 70% of the methods of contact. Mail is the 2nd most common method and is used to initiate contact that usually requests the consumer call the scammer. The internet rounds out the top three and, according to Department records, is often used as a vehicle to sell non-existing goods or develop personal relationships with the consumer in order to later ask for money.



[2] The dollar amounts represented are exclusive of any charges and fees incurred by the consumer to pay scammers through loans; withdrawals from retirement and savings accounts; necessary borrowing to replenish accounts after the consumers deplete their financial resources; and increased tax liability or Medicare premiums due to higher reported income after retirement account liquidations.

Techniques Employed by Scammers & The Financial Transactions Consumers Engage in to Pay

Scammers often deploy most if not all of the below techniques to bolster their scam.[3] Scam artists often use an official government or nationally recognized name or a variation of it to make their story seem legitimate or to confuse, or gain the trust of, consumers. Some of the most common imposter techniques scammers deploy include:

- posing as IRS agents claiming taxes are owed and threatening arrest if the taxes are not paid;
- posing as Social Security agents asking for the consumer's social security number;
- posing as Microsoft employees claiming the consumer's computer has been hacked or has a virus and offering to fix it for payments in the form of gift cards; and
- posing as the electric utility, Medicare, Publishers Clearing House, or cable/internet companies.

The communication with the consumer also frequently contains a threat (i.e., garnishment, jail) or a time sensitive request. The fraudster may also have a piece of information about the consumer derived from a security breach, social media or other venue to further aid in their ruse. This may include knowledge of who the consumer does business with, the last four digits of the consumer's social security number or the names of family members. This information allows the scammer to further gain the confidence of the unsuspecting consumer.

Consumers who fall victim empty their checking accounts, savings accounts, retirement accounts, and send saved cash to pay fraudsters and scammers. Common methods of delivery are either cash (transferred through wire transfer, money transmitters or mail) or alternative methods that spend like cash and are difficult to trace such as gift cards or pre-paid debit cards. Scammers follow the headlines and as companies and consumers become wise to the use of a certain method of payment collection, and perhaps put safeguards around their use, the thieves switch gears.

Types of Evidence to Demonstrate Loss Due to Fraud or Scam & Balancing Evidentiary Needs

As part of the ANPRM, the Administration also asked how it might revise its rules to better assist victim-beneficiaries in proving a major life-changing event (LCE) from a loss of income-producing property due to criminal fraud or theft.[4] Balancing the Administration's need for an evidentiary basis to determine the existence of a LCE and the burden such requirements place on beneficiaries means re-examining the rules in 20 CFR Section 418. For example, the current standard for proving a major LCE based on a loss of income-producing property due to fraud or theft is evidence of conviction.[5] Scammers are difficult to identify and convict; therefore, this is too high of a burden of proof for the individual beneficiary. Instead, beneficiaries could be allowed to use their own records as evidence to show that they have been victims of fraud or a scam. Such

[3] For a rundown of common scam red flags and ways to avoid them, view the Department's *Ditch the Pitch: A Guide to Guarding Against Scams* publication at https://www.consumer.sc.gov/ditch-pitch.
[4] *See* 20 CFR 418.1205*(e) and 418.2205.*
[5] *See* 20 CFR 418.1255*(e) and 418.2255.*

evidence could include phone records or other evidence of correspondence with the scammer, shipping carrier records, financial records, correspondence with financial institutions regarding the scam, gift card receipts, declarations, affidavits, police reports, scam reports, complaints, or a combination thereof.

Evidence of a major LCE is provided to support a beneficiary's request that the Administration use a more recent tax year to make a new initial determination of IRMAA.[6] The Administration could also consider adding a review opportunity for victims of scams requesting a new initial determination of IRMAA after an LCE due to fraud. The current regulations state that dismissals of a request for a new initial determination or a request for reconsideration of IRMAA are not subject to the administrative review process or judicial review.[7] This means that if the evidence provided by the beneficiary were deemed insufficient, there is no recourse. Perhaps the Administration could amend the rules to allow beneficiaries an additional avenue for review. If the Administration determines that the evidence provided by a beneficiary is insufficient to support a new initial determination of IRMAA, at a minimum, it could explain its basis and allow an opportunity for the beneficiary to submit additional information with a request for reconsideration. This added step could also ensure no mistakes or errors were made in the initial round of claim review.

Conclusion

The Department supports the Administration's objective to reform its rules to alleviate the burden on beneficiaries who fall victim to fraud or scams. We appreciate the opportunity to comment on the ANPRM and commend the Administration for the work and effort put into this process.

SCDCA hopes you find the information we provided beneficial as you decide a path forward for this proposed rule. Should you have any questions pertaining to our comments, please feel free to contact me at 803-734-4233.

Regards,

Roger Hall, Esq.
Deputy Consumer Advocate

[6] See 20 CFR 418.1310(a)(4) and 418.2310(a)(4).
[7] *See 20 CFR § 418.1301 and 2301.*