INVESTMENT COMPANY INSTITUTE®

ICI OPERATIONS

MARCH 2020

Red Flag Indicators: Warnings of Potentially Fraudulent Activity

Red Flag Indicators: Warnings of Potentially Fraudulent Activity

Contents

Introduction

As fraudsters, scam artists, criminals, and other "bad actors" continue to target the financial services industry and its customers, it is critical that mutual funds and their transfer agents implement and maintain strong fraud prevention controls and programs. A robust fraud prevention program should include multiple layers rather than relying on a single control or technical solution. The program also should evolve with new and emerging risks and schemes.

An essential layer in any fraud prevention program is the ability to identify and detect potential red flags[1] that may be indicative of fraud. The presence of a red flag does not necessarily mean that fraud is occurring, but it can be an indicator that an extra review or inspection of a transaction, call, or account may be warranted. It is critical that funds and transfer agents have a documented escalation protocol in place to address any situation where a red flag is identified.

An Investment Company Institute (ICI) industry working group developed this paper to help funds and transfer agents:

- Identify red flags that may be indicative of fraud
- Identify possible enhancements to their fraud prevention and Reg S-ID: Identity Theft Red Flag[2] programs
- Augment their internal fraud prevention training resources

The paper is intended to address indicators other than those brought to the attention of funds and transfer agents by shareholders or their advisers (e.g., suspicious or unauthorized transactions or reports of identity theft or fraud involving accounts at other financial institutions).

In addition, funds and transfer agents may use this paper to consider how technology may improve their overall fraud detection and prevention efforts, including substituting or supplementing back-end/after-the-fact controls with real-time alerts/warnings through the use of technology, augmented intelligence (AI), and automation.

To facilitate inclusion within a fund/transfer agent's training program(s), the paper can be used as a comprehensive listing of red flags; it can also be divided by customer touchpoint (e.g., call center, written communication, website), which would enable targeted training based on specific roles and responsibilities within an organization.[3]

This document is not intended to provide legal advice and should not be relied on for that purpose. It is intended only to serve as a tool to assist fund operations and transfer agent management in their independent evaluation of their fraud prevention, suspicious activity, or Reg S-ID: Identity Theft Red Flag programs.

[1] A red flag is an indicator or warning of potential suspicious activity.

[2] Adopted in April 2013, SEC Rule S-ID: Identity Theft Red Flags requires certain SEC-regulated entities to develop and implement a written program designed to detect, prevent, and mitigate identity theft in connection with certain accounts.

[3] The working group intentionally did not address red flags that may be indicative of employee fraud in this paper. The working group felt that potential employee fraud should be addressed separately with a limited, controlled distribution of any work product.

Call Center

The call center is generally a fund or transfer agent's first line of defense against fraudsters, scam artists, criminals, or other bad actors. Fraudsters tend to contact the call center multiple times before attempting a fraudulent transaction. Therefore, regular fraud prevention and red flag detection training is critical for all call center associates. A comprehensive fraud prevention training program could include a catalog of behaviors and red flags[4] that are typically associated with fraud or other nefarious behavior.

What to Listen For

Many potential red flags are easily identified by carefully listening to a caller. During a call, the following factors may be indicators of potential fraud or that the caller is an imposter or fraudster.

Voice

- The caller's voice is inconsistent with the age or gender of the shareholder as indicated by information available to the call center representative about the shareholder.
- The caller has a foreign accent inconsistent with account information on file.
- The caller uses phrases such as "I've had a tracheotomy," "I've got a bad cold today," or "I just got out of the hospital" as an explanation for any age/gender discrepancy when asked further identifying questions.
- The caller's voice sounds electronically modified or monotone with unnatural pauses.
- The caller uses a relay service for the hearing-impaired[5] to request telephone transactions.

Mannerism

- The caller sounds nervous, is evasive, acts confused, or is unable to provide sufficient information to pass the security check.
- The caller appears to be following a script.
- The caller sounds coached (or the phone representative can hear someone in the background coaching the caller).[6]
- The caller refers to himself/herself by multiple names (e.g., as the shareholder, as the shareholder's assistant, as a family member).
- The caller does not know how to pronounce the shareholder's name, street name, or city.
- The caller mixes up the shareholder's first and last name (e.g., refers to self as *Doe, John,* rather than *John Doe*).
- The caller is in a rush or seems anxious to complete a transaction quickly.

[4] The presence of one or more red flags does not necessarily mean that fraud is occurring or that the caller is a fraudster, but red flags can indicate that the fund/transfer agent may consider undertaking an extra review or inspection of a transaction, caller, or account.

[5] Relay services are telephone services that enable people who are deaf or hard of hearing, or who have a speech impairment, to communicate in a manner that is "functionally equivalent" to the ability of an individual without a disability to communicate by telephone.

[6] This may also be an indication of elder financial abuse or exploitation.

- The caller exhibits persistent behaviors (e.g., expresses urgent need to establish an Automated Clearing House [ACH] transaction[7] or liquidate funds, expresses a desire to avoid Medallion Signature Guarantee [MSG] requirements, calls frequently to confirm whether new bank information has been established and/or liquidations have been processed).
- The caller expresses excitement over a financial windfall or prize check or uses key phrases associated with common exploitation schemes (e.g., sweepstakes, lottery, real estate, home improvement).
- The caller expresses fear or anxiety over an urgent call or notice purportedly received from the Internal Revenue Service, Social Security Administration, law enforcement, or an individual demanding financial compensation for a family member in dire straits (e.g., in jail, kidnapped).

Nonstandard US English

- The caller uses a date format not typically used by US-based investors (e.g., day/month/year).
- The caller uses "kindly" instead of "please."
- The caller mischaracterizes the nature of their investment account (e.g., refers to account as a "policy," "contract," or "subscription").

Account Knowledge

- The caller does not know their account number and tries various methods to obtain the account number, including providing a Social Security number (SSN).
- The caller is unfamiliar with or does not have the identification information they are being asked to provide (e.g., not knowing their own SSN or date of birth [DOB]).
- The caller makes statements regarding identity information (e.g., SSN, DOB) that are confusing, do not make sense, or are unusual.
- The caller is unfamiliar with existing account details (e.g., email address, other shareholders on the account, address of record [AOR], account number, mutual funds the account is invested in, authorized trader's name, pre-established bank information), or recent account activity (e.g., existence of an automatic investment plan [AIP]).
- The caller is unable to answer basic out-of-wallet questions.[8]
- The caller is unable to verify additional account information (e.g., beneficiaries listed on account, bank information on file, financial adviser) upon request.
- The caller uses inappropriate or incorrect terms to describe the nature of their investment account (e.g., refers to account as a "policy," "contract," or "subscription") or guesses at the type of account (e.g., individual retirement account [IRA], Uniform Transfer to Minors Act [UTMA], trust, transfer on death [TOD]).

---

[7] ACH is a computer-based clearinghouse and settlement facility established to process the exchange of electronic transactions between participating financial institutions. In this document and the mutual fund industry, ACH is also used interchangeably to describe banking information added to an account.

[8] Out-of-wallet questions (as part of knowledge-based authentication) refer to private data used for authentication for telephone or web activities. Answers to out-of-wallet questions are typically those that are easily recallable by a user but obscure to most other persons and difficult for others to uncover.

Call Characteristics

- The incoming call is coming from a voice over internet protocol (VoIP)[9] or a blocked or unlisted phone number.
- The telephone/area code of the incoming call is inconsistent with the phone number and state on file for the account.[10] For example:
  - The incoming call is from a phone number different from what is listed on the account record.
  - The caller provides a phone number that is different from what is displayed on the call identification screen.
  - The call is coming from an area code outside of the shareholder's state or country of residence as listed on the account.
- A bad telephone connection (e.g., audible clicking noises in the background) may indicate an internet or overseas routed call or a delayed response due to latency in a VoIP line.
- There is audible background noise (traffic, public address announcements) that appears inconsistent with someone calling a financial institution regarding sensitive personal information.
- There is a lag between the time the phone representative asks a question and when the caller responds, which may indicate:
  - The caller is shuffling through papers to find answers to questions they should know (e.g., their own DOB or phone number).
  - The caller is typing in the background, especially when asked identifying information (may indicate that they are looking up information online or within a database of stolen personal information).

What to Look For: General Behavior

It can be difficult to identify red flags solely on the basis of a conversation with a caller. In addition to the factors outlined above, certain behaviors on their own or in conjunction with the history of the shareholder account may be indicators of potential fraud or that the caller may be an imposter. Call center representatives may consider the following factors when evaluating a caller or transaction for potential fraud:

- The caller has failed the required security check(s) or authentication process multiple times (this may occur over the course of several calls).
- The caller does not exhibit concern when the phone representative is unable to locate an account registered to the caller.
- The caller provides multiple SSNs when attempting to locate an account (e.g., presents various SSNs for a spouse, child, parent).
- The caller refuses or is hesitant to provide a phone number, provides an invalid phone number or a phone number that is disconnected, or states that they will call the call center back at another time.

[9] VoIP stands for voice over internet protocol and refers to a methodology and group of technologies for the delivery of voice communications and multimedia sessions over internet protocol (IP) networks. Skype, Vonage, YMAX, GoTextMe, Enflick, Bandwidth/CLEC, Google/Bandwidth, Neutral Tandem, and TextPlus are examples of VoIP providers.

[10] In some cases, the area code for the phone number may not match the address/state on file because the caller is using a cell phone or a landline carried through a cable/internet provider.

- The caller provides a call-back number that does not match the phone number on file.[11]
- The caller refuses to be transferred to a dedicated service team when offered that opportunity.
- The caller disconnects when unable to pass additional authentication protocols.
- The caller provides personal information that is inconsistent with other information provided previously for the account.
- The caller contacts the call center multiple times (in one day or over a short period of time) with questions regarding processing requirements, account rules, redemption maximums, MSG requirements, or how to add new bank account information to an account.
- The caller requests an exception to processing requirements, claiming that all necessary processing requirements were not provided to them previously.
- The caller acts as if they cannot hear the phone representative to buy time while looking up or searching for identifying information.
- The caller insists that a redemption be processed as soon as possible and is uninterested in using the redemption options currently available on the account (e.g., by check to the address of record or to the existing bank on file).
- The caller requests that a redemption check be sent overnight or as quickly as possible without a valid explanation, or they provide an elaborate or illogical explanation.
- The caller calls multiple times to check on the status of a redemption check being sent via overnight delivery and is insistent that a tracking number be provided for the overnight package.
- The caller probes for ways to avoid any MSG requirements without stating why they are unable to obtain an MSG.
- The caller requests multiple redemptions within days of each other without regard to market value and/or fees.
- The caller asks questions regarding how quickly a redemption can be made to a new bank account.
- The caller requests service forms or bank change forms be sent to an email address unrelated to the account or to an address that is not on file.
- The caller wishes to engage in transactions that lack business sense or an apparent investment strategy.
- The caller exhibits a lack of concern regarding any commissions (e.g., contingent deferred sales charge), other transaction costs, or any possible tax consequences tied to a redemption (e.g., an early redemption from an IRA or retirement plan subject to withholding).
- The caller exhibits unusual concern for secrecy, particularly with respect to his/her identity, type of business, assets, or dealings with firms.
- The caller is overly concerned about the fund company's compliance with reporting requirements with respect to validating their identity or type of business.
- The caller gives instructions that appear improper or do not "add up."

[11] This could be a legitimate situation where the shareholder is providing their cell phone number or a landline carried through a cable/internet provider.

What to Look For: Account History

- Memos or notes indicating that the fund/transfer agent has been notified of unauthorized activity or transactions within the shareholder's account, that the shareholder has not been receiving account statements, or that the shareholder is a victim of identity theft or other fraud
- Recent financial (e.g., redemptions, transfers) or maintenance (e.g., change of address or email address, change of document delivery method to email) transactions
- A request to add a new secondary/alternate address or alternate payee to an account
- An address change (postal or email) or a change in account credentials closely followed by a large redemption, redemption request, or request for online access
- Multiple address change requests in a short period of time
- A request to update the address of record to a country other than the United States
- Use of suspicious or unusual email names/addresses/domains associated with an account.

Examples of unusual email domain names include (but are not limited to):

- @mail.com
- @homeemail.com
- @artlover.com
- @uymail.com
- @reggaefan.com
- @acdcfan.com
- @yandex.com
- @yopmail.com
- @opayq.com
- @vfemail.net
- @guerrillamail.net
- @guerillamail.biz
- @guerillamail.com
- @temp-mail.org
- @wiseyoho.com
- @babatfirst.com
- @myyou.com

Examples of unusual email usernames include:

  - Username begins with "doctor" plus 4 numbers (e.g., doctor8877@, doctor7878@).
  - Username contains a variation of USSERVICE (e.g., usservice@, usservicenow@, usservice101@).
- A request to add new bank information to the account shortly after account opening
- Requests to change or add new bank information followed shortly by requests for one or more redemptions
- Multiple requests to stop and reissue outstanding checks, followed by a request to cancel the redemptions altogether
- A noticeable change in the shareholder's normal pattern or history of transactions (e.g., a previously dormant account with multiple recent transactions)
- Requests made beyond legal authority of fiduciary (e.g., power of attorney [POA], guardian, conservator, corporate officer)
- A request for online access or password resets that are out of character with previous shareholder activity/ requests (e.g., based on age of shareholder, or no history of online activity)[12]
- Purchases received from what appears to be an unrelated third party

Questions Related to Specific Transactions That May Indicate Fraud

Fraudsters often contact the call center to gain an understanding of processing requirements and loopholes to exploit. They do so by making multiple calls and asking a series of questions to acquire an understanding of fund policies, such as check hold periods, MSG requirements, and other fraud prevention controls. Frequently, they "answer shop" until they find an overly helpful call center representative and obtain the information they are seeking. Though the questions themselves may not be suspicious, they may be indicators of fraud when considered in conjunction with the other red flags outlined within this document. Examples of questions that fraudsters may ask include (but are not limited to):

Bank Information on File

- How quickly can I add or change a bank account tied to my account?
- Is there a wait period before I can send money to a new bank account?
- Why do I need an MSG to add new bank information to my account?
- Can I add a debit card as my bank of record?
- Can I fax the information to add bank information to my account?
- Can you waive the waiting period to use a new bank on file? (Often the caller will be extremely persistent.)

[12] This may be indicative of an account takeover by a fraudster.

Check Writing

- Which of your funds offer check writing?
- How soon can I receive a checkbook?
- Can a checkbook be sent to me via overnight delivery?
- Can a checkbook be issued if there is no money invested in my account?
- Is there a limit on the number of checks I can write?
- How many checkbooks can I request at one time?
- Can I order my checkbook online or from some other vendor?

Investment Checks

- Do you accept starter checks?
- Do you accept corporate checks?
- Do you accept third-party checks?
- What is your hold period on new purchases before I can take money out of my account?
- Under what situations will that hold period be waived?
- Can I endorse a check made payable to me (e.g., second-party check) over to the fund?

Red Flags in Combination May Indicate a Higher Risk of Fraud

Situations where more than one red flag is present are often indicative of a higher probability of fraud or that the caller may be an imposter. Some common examples of combinations of red flags that may be indicative of fraud include (but are not limited to):

- A call where:
  - the caller speaks in a computer-generated voice; and
  - the telephone number of the caller is not tied to the shareholder or account; and
  - the caller requests a telephone redemption.
- A call where:
  - the shareholder has been reported deceased, and
  - the caller purports to be the shareholder and requests a telephone redemption or any other change to the account.
- A call where:
  - there is a recent addition/update to the bank instructions on the account; and
  - the caller requests a telephone redemption; and
  - the caller requests that the redemption be expedited.

- A caller who:
  - speaks in nonstandard English and/or with a distinct foreign accent that is inconsistent with the account information on file, and identifies as the owner of an account with a US address of record; and
  - cannot confirm the account number/SSN on file; and
  - asks questions about wiring redemption proceeds overseas; and
  - asks if redemption requests can be faxed after being told that request must be in writing.
- A caller who:
  - is unable to pronounce the name of a shareholder (their own name or the name of a joint owner) or street address on file; and
  - has trouble passing standard authentication questions; and
  - requests a telephone redemption.
- A caller who:
  - claims to be a financial adviser; and
  - cannot provide account numbers but requests confirmation that one or more individuals have an account with the fund family.

Processing

Fraudsters, scam artists, or other criminals often seek to defraud shareholders by contacting the fund/transfer agent via written requests or by facsimile/fax. Associates responsible for handling such requests play a critical role in identifying and preventing fraud from occurring. As with the call center, regular fraud prevention and red flag detection training is imperative for all associates who handle or process written transactions.

As an initial step in identifying potential fraud, processors should review all documents provided to ensure that everything is in "good order" and meets all processing requirements. Processors should also review the account for any memos or notes indicating that the fund/transfer agent has been notified of unauthorized transactions within the shareholder's account, or that the shareholder has not been receiving account statements or is a victim of identity theft or other fraud. Red flags[13] that processors are more likely to encounter and that funds/transfer agents may consider including in their training programs include:

What to Look For: Overall

- The request has typos, spelling mistakes, grammatical errors, and phrases that do not make sense or are unusual for a US investor.
- Written requests have poor grammar.
- The request uses "kindly" or other nonstandard English phrases in written communication.

[13] The presence of a red flag does not necessarily mean that fraud is occurring or that the requester is a fraudster, but one or more red flags may indicate that the fund/transfer agent may consider undertaking an extra review or inspection of a transaction, caller, or account.

- The identifying information is inconsistent with other readily available data.
- Documents provided for identification appear to have been forged or altered.
- Documents received appear to be copies, altered, forged, or have the appearance of having been destroyed and reassembled.
- The MSG, notary stamp, or enclosed check drafts appear to be copies.
- The information provided for identification is inconsistent with readily accessible information on file with the transfer agent (e.g., signature card, recent check).

What to Look For: New Account Applications/New Purchases

- The address on the purchase check is different from the address on the application.
- The application does not list a financial adviser or a designated dealer of record.
- The address listed on the application is a suite, PO box, or drop box.
- The mailing address on the application contains misspellings.
- The shareholder's name is misspelled or different in other sections of the application.
- The SSN/Tax Identification Number (TIN) or DOB is different in other sections of the application.
- The four required Customer Identification Program (CIP) elements (name, SSN, DOB, residential address) are missing, incomplete, or incorrect.
- Proper documentation required for an account being opened by an entity or non-natural person (e.g., articles of incorporation provided with a corporate account) is missing, incomplete, incorrect, or appears to be fraudulent.
- The application contains unusual or conflicting instructions (e.g., request for a systematic withdrawal plan [SWP] and AIP, dividends to be reinvested and an alternate address for dividend payments, every fund selected).
- The SSN provided is the same as that submitted by other persons opening an account or other customers who hold accounts with the fund complex.
- The notary stamp, MSG stamp, and/or voided check accompanying the application appears to be a photocopy.
- A joint tenant application received for an existing shareholder includes a second, new tenant who appears to be unrelated to the existing shareholder.
- The form of payment accompanying the application is unacceptable (e.g., nonbank money order, traveler's check, credit card convenience check, starter check, or a third-party check).
- The application is accompanied by a tax refund check and/or second- or third-party check.[14]
- A new account application received for an existing shareholder contains information that does not match the current information on file for the shareholder (e.g., different address, phone number, email address, bank account information).

[14] Stolen tax refund and other checks are often altered and used to fund new accounts. These fraudulent accounts are opened using the names and SSNs of identity theft victims but often include an address belonging to the fraudster.

- The new account is being funded with a check drawn off an account belonging to someone other than the shareholder.
- The new account application lacks business sense or an apparent investment strategy (e.g., looks to invest in multiple single-state tax-exempt funds outside of the applicant's state of residence).

What to Look For: Purchases

- The purchase check received contains signs of alteration, such as:
  - Uneven shading of borders
  - Blurry/fuzzy or cutoff corporate logos or authorized signature(s)
  - Misspellings or typos in the customer registration, address, or elsewhere on the check
  - Poor or unusual formatting of customer registration
  - Missing key information on the check (e.g., ABA[15] or bank routing number, bank account number)
  - Poor or unusual formatting of the ABA number or magnetic ink character recognition (MICR) line[16]
  - Altered ABA number or MICR line
  - An incorrect fractional routing number (e.g., the fractional number in the upper right-hand corner of the check) that does not match the ABA routing number and physical location code of the bank when "decoded"[17]
  - Font inconsistencies, including multiple differing font types or sizes (may indicate check is computer-generated)
  - Missing check perforations (may indicate check was printed on a laser printer)
  - Missing standard security measures (e.g., security bands, watermarks), which indicate that the check is a photocopy
  - Check appears to have been washed (e.g., payee information and/or dollar amounts appear to be erased and rewritten)
  - Standard or odd-colored paper rather than typical check stock
- The first purchase into the account from a recently added bank (ACH transaction) is rejected, and it can be confirmed that the reject is not a result of a processing error (e.g., a typo).
- The account history shows an excessive number of returned ACH drafts and/or returned deposits.
- A corporate check is used to make a purchase into a non-related account or an account registered to an individual.

---

[15] In the United States, an ABA routing number is a nine-digit code printed on the bottom of checks to identify the financial institution on which it was drawn.

[16] MICR is technology used by banks to make the processing of paper checks easier. The MICR line is a row of numbers/characters at the bottom of a paper check that provides information about the account the check is drawn on and is in a very specific font.

[17] More information regarding fractional routing numbers is available at https://help.cubase.org/cubase/recognizing_a_fraudulent_check.htm. Information regarding decoding a fractional routing number is available at www.wikihow.com/Calculate-the-Check-Digit-of-a-Routing-Number-from-an-Illegible-Check.

- The purchase is made by a third-party check or a third-party check with different first or last names from the account holder's.
- The purchase is made using a starter check.
- The purchase is made using a convenience (credit card) check.
- The request to add bank information includes a 16-digit or longer-than-normal bank account number, which may indicate that it is associated with a prepaid debit card.
- The purchase is made using cash equivalents (i.e., money order, traveler's check).
- The purchase is coming from a foreign financial institution or is in a foreign currency denomination.
- The first purchase into the account is made via a high-dollar ACH draft.

What to Look For: Redemptions

- A request for an expedited redemption is made through an online fax service (e.g., eFax, HelloFax, MyFax, SmartFax).
- The redemption request includes a suspicious signature(s) (e.g., does not match signatures on previous requests, the original account application, or check-writing card).
- Liquidation or dividend/capital gain proceeds sent to newly added ACH instructions are rejected by the bank, and it can be confirmed that the reject is not a result of an input error.
- There have been frequent requests to change the payment method (e.g., multiple ACH instruction changes or requests to send proceeds via mail to the address of record when there are bank instructions on file).
- A redemption request received shortly after a recent purchase clears the required escrow hold period, but the request asks for the proceeds to be sent to a new bank other than the bank on file (where the initial purchase originated) or to be sent in an expedited fashion.
- A redemption request to wire/transfer the funds to a third party or firm immediately follows a recent purchase.
- A redemption request asks that redemption proceeds be wired to a foreign person or country/destination (e.g., Asia, Nigeria, Russia, China).
- A redemption request is made payable to an unrelated third party or sent to a suspicious address, especially when following a recent purchase.
- A redemption request seeks a full or substantial redemption within 30 to 60 days of account opening or of the initial purchase.
- A redemption request is received following multiple inquiries (e.g., phone, website, email, chat) regarding the account.
- A redemption request is received following a change of account contact information (e.g., phone number, physical address, email address).
- A redemption request includes an MSG that fails the verification process (e.g., ink or barcode is invalid; prefix is inconsistent with dollar amount of the request; MSG has been reported as lost or stolen;[18] signature is missing).

[18] Lost or stolen MSG stamps are listed within Kemark's database (www.kemark.com).

- The redemption request appears to have been altered or has sections redacted or "whited out."
- The redemption request includes questionable or suspicious documents (e.g., legal documents that appear to have been altered).
- The redemption request contains different handwriting in various sections.
- Account memos, entries, or stop codes tagged to an account indicate negative activity, or there is notification of incapacity, notification of identity theft, or recently returned mail.
- The redemption request shows a disregard for penalties, fees, or other transaction costs.
- The account has had multiple recent changes to key contact information (e.g., address, phone number, email address).
- A redemption request is received for an account that has a history of extensive wire activity or wire transfers.

What to Look For: Faxes

- A fax request is received through an online fax service such as eFax, HelloFax, MyFax, or SmartFax.
- The incoming fax number/area code is inconsistent with the address or phone number on file for the shareholder (e.g., fax is received from an area code outside of the shareholder's state or country of residence).
- An attempt is made via fax to add or change bank instructions in conjunction with other red flags outlined.
- The telephone number included on the fax request for callbacks does not match the telephone number[19] on file with the fund/transfer agent for the account.
- The signature included on the fax request does not match the signature on file with the fund/transfer agent for the account.
- The fax includes a font designed to appear as handwritten, and the signature is electronic or in a font meant to imitate a handwritten signature.
- The request or the signature includes improper use of capitalization and/or inappropriate spacing.
- The fax appears blurry, fuzzy, crooked, or cut off.
- The fax includes the use of "kindly" or other nonstandard English phrases in the text.

What to Look For: Adding/Changing Bank Information

- The voided check or check draft provided to establish bank instructions contains typos, spelling mistakes, grammatical errors, and phrases that do not make sense or are unusual for a US investor.
- The voided check or check draft provided to establish bank instructions includes:
  - Inconsistencies with the customer name or address listed on the application or on file
  - Poor or unusual formatting of customer registration
  - Blurry/fuzzy, cutoff, crooked, or out-of-date corporate logos

[19] It could be a legitimate situation where the shareholder is providing their cell phone number instead of their landline number that is on file with the fund/transfer agent.

- Missing key information on the check (e.g., ABA number, bank account number)
- Poor or unusual formatting, including nonstandard font, of the ABA number or MICR line
- Altered ABA number or MICR line
- An incorrect fractional routing number (i.e., the fractional number in the upper right-hand corner of the check) that does not match the ABA routing number and physical location code of the bank when "decoded"[20]
- Appears to be a photocopy or a picture of a check
- Font inconsistencies, including multiple differing font types or sizes (may indicate check is computer-generated or printed from the web)

- A starter check is provided to initiate or establish new bank instructions on an account.
- A request to add bank information is received for an account that recently opened.
- The ABA number on the voided check or check draft belongs to a prepaid debit card or a Green Dot bank.[21] A bank account number that is 16 digits or longer than a normal bank account number may indicate that it is associated with a prepaid debit card. The following ABA numbers are currently tied to a Green Dot bank (this is not an all-inclusive list):
  - 0611 2000 0
  - 0960 1741 8
  - 1240 8502 4
  - 1243 0252 9
  - 1243 0132 0
  - 1243 0316 2 (associated with GoBank)
  - 1243 0312 0
  - 0739 7218 1 (associated with MetaBank)
- The address on the voided check provided to establish new bank instructions is different from the address on file for the shareholder(s).
- The signature on the request to add bank information is different from the signature on file with the fund/transfer agent (e.g., provided on new account application or other document).
- A maintenance request to add or change bank information on file is received for an account that has had a recent change of address, phone number, or email address, or the bank information change request includes a change to the address, phone number, or email address.
- The names provided as the bank account owner(s) on the maintenance request do not match the registration listed on the voided check included with the request.

[20] More information regarding fractional routing numbers is available at https://help.cubase.org/cubase/recognizing_a_fraudulent_check.htm. Information regarding decoding a fractional routing number is available at www.wikihow.com/Calculate-the-Check-Digit-of-a-Routing-Number-from-an-Illegible-Check.

[21] Green Dot banks are an online banking solution that may be associated with prepaid debit cards. Green Dot prepaid debit cards allow customers to transfer balances from other third-party entities (including other financial entities such as mutual funds) directly to the debit card. Prepaid debit cards tied to Green Dot banks are a preferred mechanism for fraudsters to quickly transfer money.

- Multiple maintenance requests within a short time period ask that different banks/credit unions be added to an account, especially if the requests are received via fax or email and do not include the required notary, signature verification program (SVP) stamp, or MSG stamp.
- The request to add bank information includes a letter from the bank branch manager in lieu of a voided check, and the address of the branch on the letterhead does not match the state in which the shareholder resides.
- The request to add bank information includes a notary stamp from a state different from shareholder's state of residence.
- The branch location of the bank/credit union noted on the voided check or deposit slip provided is in a different state than the shareholder's residence.
- A request asks to add an alternate payee/address or new bank instructions that involve a foreign country or high-risk location.
- A request to add an alternate payee/address or new bank instructions includes names or third parties that are unrelated or inconsistent with the shareholder(s).
- Certain authentication response codes (e.g., account status, insufficient funds, customer authentication failed, negative data [e.g., fraud flag exists]) related to the bank account on file are returned by a third-party bank validation software program.
- The bank account number provided on the request was used in a previous fraud case.

What to Look For: Maintenance Requests

- The signature(s) on the maintenance request is inconsistent with prior signatures received from the shareholder(s) (e.g., on account application, purchase checks).
- The request is missing a required notary stamp, SVP stamp, or MSG.[22]
- A maintenance request is received for an account that recently had online access activated.
- A maintenance request is received for an account that has had a recent change to the "trusted contact."[23]

What to Look For: Check-Writing Privileges

- The application for check writing is for multiple funds and accounts.
- The application for check writing has multiple registration types selected (e.g., joint tenancy, trust, UTMA).
- The application for check writing is received for an account that has not designated a broker-dealer or for an account without a named broker-dealer of record.
- The application for check writing is received for an account that has not yet been funded.
- The request for check writing is received shortly after a change of address occurs on the account.

[22] Processing requirements may vary by fund complex.

[23] The trusted contact is a person the shareholder has authorized the mutual fund/transfer agent to contact when fraud or financial exploitation is suspected, or the mutual fund/transfer agent has deemed an account to be lost under state escheatment laws.

Red Flags in Combination May Indicate a Higher Potential of Fraud

Situations with more than one red flag are often indicative of a higher probability of fraud or that the person submitting the request may be a fraudster. Some common examples of combinations of red flags that may be indicative of fraud include (but are not limited to):

- A recently opened account funded by an ACH purchase where:
  - a request to add or change banking information is received; and
  - a request for an expedited redemption is received or a request to waive the hold period accompanies the redemption request.
- Redemption or transfer request for an account that has a stop restriction due to potential fraud/death/divorce/pending legal action where:
  - instructions are not signature guaranteed; and
  - the request is missing or includes invalid documentation for resolving the stop restriction.
- New account application where:
  - no is broker listed; and
  - ACH debit is used to fund the account; or
  - the investment check is drawn against a corporate account made payable to an individual.

Web

Fraudsters, scam artists, other criminals, or "bad actors" frequently contact the fund/transfer agent via the internet using the fund's website or an online portal. When fraudsters contact the fund/transfer agent via the web, associates responsible for reviewing web activity in conjunction with various technical tools are critical to stopping fraud from occurring. As with the call center and processing departments, regular fraud prevention and red flag detection training is imperative for all associates who are responsible for reviewing web activity. Associates responsible for reviewing web activity are more likely to detect a particular set of red flags,[24] including:

Access Origination

- An individual attempts to log in with an unfamiliar or unbound[25] device.
- The IP address[26] used to access the fund's website has not been previously associated (i.e., bound) with the shareholder or account.

[24] The presence of a red flag does not necessarily mean that fraud is occurring or that the requester is a fraudster, but one or more red flags can indicate that the fund/transfer agent may consider undertaking an extra review or inspection of a transaction, caller, or account.

[25] Device binding allows users to transact on trusted devices without repetitive authentications. Device binding can occur through reliable and consistent verification of the transacting device by registering the device and binding it with a user credential. It also can bind a SIM card to a transacting device.

[26] An internet protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the internet protocol for communication.

- The IP address is associated with previous fraudulent activity.
- The "fingerprint" of the device used for online access contains one of the following suspicious elements:
  - The device is unbound.
  - The device/IP address is part of a known offender list.[27]
  - The device/IP address is coming from a TOR network.[28]
  - The device's IP address is associated with a geolocation[29] that is deemed to be high-risk (e.g., Iran, North Korea, Nigeria, Russia, China).
  - The transaction is transmitted by an aggregator device.[30]
  - The time zone associated with the IP address does not match the time zone of the shareholder's address of record.[31]
- Login attempts come from dramatically different geolocations at the same time or very close together.
- A long-standing account that has not previously had online access enabled has an online profile established. This is particularly concerning if the account is held by an elderly investor.[32]
- A new online profile is established for an existing account; the "shareholder" successfully passes authentication; and updates their banking profile. User then initiates a transaction.

Online Login Process

- An individual uses the "forgot username" or "forgot password" protocols to gain online access to an account via a suspicious IP address.
- An authenticated user attempts to enroll/modify their two-factor authentication method[33] via a suspicious IP address.
- Multiple login attempts fail to gain online access to an account.
- Multiple requests are made to reset or change the online username and/or password associated with an account.
- User fails multiple times to pass the "out-of-wallet" or challenge questions that are presented when resetting or changing a password.

---

[27] Funds may create their own internal list of suspicious IP addresses, use a third-party vendor's list, or combine both.

[28] TOR is free and open-source software for enabling anonymous communication.

[29] Geolocation is mapping of an IP address or MAC address to the real-world geographic location of an internet-connected computing or mobile device. Geolocation can be manipulated to appear to be coming from somewhere it is not; therefore, funds/TAs need to be careful when using geolocation as a stand-alone red flag.

[30] A financial data aggregator is a service that allows a consumer to store all their financial information online in one place. In March 2019, FINRA issued an Investor Alert outlining the dangers of using a financial data aggregator: www.finra.org/investors/alerts/be-mindful-data-aggregation-risks.

[31] Geolocation can be manipulated to appear to be coming from somewhere it is not; therefore, funds/TAs need to be careful when using geolocation as a stand-alone red flag.

[32] The SEC and FINRA define elder and vulnerable adults as customers who are aged 65 and older as well as those who are aged 18 or older and who, the financial institution reasonably believes, have a mental or physical impairment that prevents them from protecting their own interests. Individual states may have slightly different definitions for who is considered an elder investor (e.g., age 60 versus 65).

[33] Multifactor authentication is a method of confirming a shareholder's identity. A user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

New Account Opened Online

- Poor grammar is used in responses provided in required fields.
- No designation of a financial adviser or outside dealer of record is provided.
- A residential address is not provided or the address provided is not a legitimate residential address.
- The general information (e.g., shareholder name, address) contains misspellings.
- The shareholder's name is entered inconsistently in various required fields.
- The fields required as part of the onboarding process contain unusual or conflicting instructions (e.g., request for SWP and AIP, dividends to be reinvested and an alternate address for dividend payments, every fund selected, inconsistent selection of share classes).
- A new account is opened online with an unusually high dollar amount as the initial purchase.

General Activity Online

Bank Information

- New bank information or a change of existing bank information is provided shortly after account opening, in particular when followed by a redemption request.
- The ABA number provided to add or change bank information belongs to a prepaid debit card or a Green Dot bank. The following ABA numbers are currently tied to a Green Dot bank (this is not an all-inclusive list):
  - 0611 2000 0
  - 0960 1741 8
  - 1240 8502 4
  - 1243 0252 9
  - 1243 0132 0
  - 1243 0316 2 (associated with GoBank)
  - 1243 0312 0
  - 0739 7218 1 (associated with MetaBank)
- The request to add bank information includes a 16-digit or longer-than-normal bank account number, which may indicate that it is associated with a prepaid debit card.
- A maintenance request to add or change bank information on file is received for an account that has had a recent address, phone number, or email address change.
- A request is made to add to an account an alternate payee/address or new bank instructions that involve a foreign country or high-risk location.
- An authenticated user attempts to add new bank information unsuccessfully.

Financial Transactions

- Frequent online purchases are followed by redemptions of the same amount within a short period of time.
- Online purchases are made at or just below the maximum dollar amount allowed online via ACH over the course of several days.
- An online redemption request is received immediately after or within a few days of an online purchase transaction.
- Online redemption requests for or just below the maximum dollar amount are received over the course of several days.

Nonfinancial Transactions

- Address change is made online, followed within a short period of time by an online redemption or a redemption request submitted via the call center.
- Change in banking information or address processed online is followed by subsequent calls to the call center inquiring how/when a redemption can be requested.
- Change in document delivery preferences to e-delivery is followed by a change in contact information (e.g., physical address, email address, phone number) and/or a redemption request.
- Change in an email address is followed by additional changes in contact information (e.g., physical address, phone number) and/or a redemption request.
- Change in email address is followed shortly by a password reset.

Web Chat/Email Correspondence

Fraudsters, scam artists, other criminals, or "bad actors" frequently contact the fund/transfer agent via email or web chat (if offered) as a means to maintain some level of anonymity. When fraudsters contact the fund/transfer agent via email or web chat, associates responsible for responding to or reviewing the emails or chats are critical to stopping fraud from occurring. As with the call center and processing departments, regular fraud prevention and red flag detection training is imperative for all associates who are responsible for responding to and/or reviewing email and web chat. Associates responsible for reviewing web chats or emails are more likely to detect a particular set of red flags,[34] including:

What to Look For: Overall

- The correspondence contains typos, spelling mistakes, grammatical errors, or phrases that do not make sense or are unusual for a US investor.
- The word "kindly" is used in written communication.
- The individual appears to be phishing for information that should already be known to the shareholder.

[34] The presence of a red flag does not necessarily mean that fraud is occurring or that the requester is a fraudster, but one or more red flags can indicate that the fund/transfer agent may consider undertaking an extra review or inspection of a transaction, caller, or account.

- The individual is reluctant to contact client services or speak to a person and prefers to communicate only via web chat or email.
- The individual provides a "sob story" or elaborate reason why they are unable to comply with the necessary processing requirements, or why they need a redemption processed immediately.
- The individual refuses to provide his/her contact information.
- The individual makes a request that is unusual/out of the ordinary, or requests sensitive or personal information.
- The individual communicates from or asks for information to be sent to an email address not associated with the account.

Nonstandard US English

- The individual uses a date format not typically used by US-based investors (e.g., day/month/year).
- The individual mischaracterizes the nature of their investment account (e.g., refers to account as a "policy" or "contract").
- The individual lacks understanding of or guesses at the type of account (e.g., IRA, UTMA, trust, TOD).
- The word "kindly" is used in written communication.

Unusual Email Domain or Usernames

- Use of suspicious, disposable, or unusual email names/addresses/domains associated with an account. Examples of unusual email domain names include (but are not limited to):
  - @mail.com
  - @homeemail.com
  - @artlover.com
  - @uymail.com
  - @reggaefan.com
  - @acdcfan.com
  - @yandex.com
  - @yopmail.com
  - @opayq.com
  - @vfemail.net
  - @guerrillamail.net
  - @guerillamail.biz
  - @guerillamail.com
  - @temp-mail.org
  - @wiseyoho.com
  - @babatfirst.com
  - @myyou.com

Examples of unusual email usernames include:

- Username begins with "doctor" plus 4 numbers (e.g., doctor8877@, doctor7878@).
- Username contains a variation of USSERVICE (e.g., usservice@, usservicenow@, usservice101@).

Back-End Monitoring

The strongest fraud prevention programs are based on a layered approach using multiple tools and resources to identify and prevent potential fraud. Though many red flags may be identified in real time, it is important that funds and transfer agents also establish a series of back-end reports to identify red flags that may have been missed in real time or that cannot currently be identified in real time. When determining what types of back-end reporting are appropriate, funds/transfer agents could consider the following factors:

- **Intersection of fraud and anti–money laundering (AML).** Consider any crossover or duplication between reports designed to identify potential fraud and those implemented under the fund's AML program to identify suspicious activity and ensure that appropriate personnel are reviewing the applicable reports. The reports outlined in this section are intended to address potentially fraudulent activity only and are not meant to replace any reports designed in response to applicable AML/CIP regulations.
- **Coordination across the organization.** Reports described in this section may be the responsibility of and/or reviewed by different parts of an organization (rather than a specific fraud prevention function). Therefore, there should be coordination between the reviewer of a particular report and those responsible for fraud prevention or monitoring to ensure communication and sharing of information is occurring between departments.
- **Age of shareholder as a review factor.** Funds/transfer agents could consider including an age-based component to any report they develop, as the shareholder's age may be a consideration when evaluating any red flag alert.
- **Looking to the future.** Funds/transfer agents (TAs) should be looking to the future when developing any type of back-end reporting, including:
  - identifying which back-end monitoring reports could be replaced with real-time alerts using technology such as existing voice response units, AI, or robotics;
  - identifying how technology such as AI can be used to develop new reports to identify combinations of red flags, especially across customer touchpoints (e.g., call center, web); and
  - periodically evaluating the effectiveness of reporting.

Back-end monitoring reports that funds/TAs may consider implementing include (but are not limited to):

Online Access

- A report that identifies the following:
  - An individual using the "forgot username" or "forgot password" protocols to gain online access to an account via a suspicious IP address
  - An authenticated user attempting to enroll/modify their two-factor authentication method[35] via a suspicious IP address
  - Multiple failed login attempts to gain online access to an account
  - Multiple requests to reset or change the online username and/or password associated with an account
  - Multiple failed responses to out-of-wallet or challenge questions presented when an individual is resetting or changing a password
- A report that identifies the following:
  - Attempts to log in with an unfamiliar or unbound device
  - IP addresses used to access the fund's website that have not been previously associated (i.e., bound) with a specific shareholder or account
  - Occasions where the fingerprint of a device used for online access contains one of the following suspicious elements:
    - The device/IP address is part of a known offender list.
    - The device/IP address is coming from a TOR network.
    - The device's IP address is associated with a geolocation that is deemed to be high-risk (e.g., Iran, North Korea, Nigeria, Russia, China).
    - The transaction is transmitted by an aggregator[36] device.
    - The location associated with the IP address does not match the ZIP code of the shareholder's address of record.
    - The time zone associated with the IP address does not match the time zone of the shareholder's address of record.
- A report identifying when an online profile is established for the first time on a long-standing account that has not previously had online access enabled (in particular if the account is held by an elderly investor)

[35] Multifactor authentication is a method of confirming a shareholder's identity. A user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

[36] A financial data aggregator is a service that allows a consumer to store all their financial information online in one place. In March 2019, FINRA issued an Investor Alert outlining the dangers of using a financial data aggregator: www.finra.org/investors/alerts/be-mindful-data-aggregation-risks.

- A report identifying when a new online profile is established for an existing account, and the "shareholder" successfully passes authentication, updates their banking profile, and initiates a transaction
- A report identifying all newly established web access accounts with a change of password, change of bank information, or a redemption within a six-month period
- A report that identifies attempts to access an account online where the owner is deceased

New Accounts

- Account ownership information (e.g., name, SSN, Employer Identification Number, DOB, residential address) that does not match external or internal sources used for CIP or fraud detection. For example:
  - The address does not match any addresses found in third-party databases.
  - The address does not match the shareholder's credit history.
  - The SSN provided has not been issued, is listed on the Social Security Administration's Death Master File, or is listed as belonging to another individual.
  - The DOB does not match the DOB associated with that individual in third-party databases.
  - There is a lack of correlation between the SSN issuance time frame and the shareholder's DOB.
- New accounts opened within a short period of time with the same address of record and similar characteristics as unrelated other accounts (e.g., bank account, check issuer/format, account options selected)
- New accounts opened with an SSN that is associated with other unrelated persons/accounts within the fund complex
- New accounts opened online with an unusually high dollar amount as the initial purchase, especially if it is made via ACH
- Newly established accounts without a financial adviser or outside dealer of record listed
- New accounts opened with a suite, PO box, drop box, or a business location listed as the residential address of record
- New nonretirement accounts opened that have not yet been funded
- New accounts opened with a foreign address as the address of record
- New accounts using key information (e.g., name, DOB, SSN) associated with previous fraud incidents or suspected fraud investigations

Financial Transactions

- Redemptions processed within a specified period after a bank account change
- Previously inactive accounts that suddenly have redemption or transfer activity
- Accounts that have ACH purchase(s) of various amounts followed by a redemption or a series of redemptions
- Specific transaction types (e.g., redemptions) exceeding a specified dollar threshold
- Accounts with an address of record outside the United States that had recent transaction activity
- Redemptions processed shortly after a purchase cleared any required escrow hold period
- Redemption requests received immediately after or within a few days of a purchase processed via federal funds wire
- Redemptions processed shortly after an ACH purchase where the redemption proceeds are being sent via ACH to a bank other than the bank from which the initial purchase originated
- Redemptions processed shortly after a purchase where the redemption proceeds are being sent to a bank that was previously not on file
- Redemptions preceded by two or more maintenance change requests (e.g., address, email, or telephone number change; banking instructions added; and/or online access established)
- Purchase (in particular those via ACH) or redemption requests at or just below the maximum dollar amount allowed over the course of several days
- Redemption requests to wire redemption proceeds to a foreign person or high-risk country/destination (e.g., Asia, Nigeria, Russia, China)
- Redemption requests made payable to an unrelated third party or sent to a suspicious address, especially when following a recent purchase
- Requests for a full or substantial redemption within 30 to 60 days of account opening or the initial purchase
- Redemption requests received following multiple inquiries (e.g., phone, website, email, chat) regarding the account
- Redemption requests received following a change of account contact information (e.g., phone number, physical address, email address)
- Activity in an account that is inconsistent with previously established patterns of activity for that type of account

Adding/Changing Bank Information

- Addition of or change of bank information on file on an account that has had a recent address, phone number, or email address change
- Addition of an alternate payee/address or new bank instructions that involve a foreign country or high-risk location
- Authenticated user attempts to add new bank information online unsuccessfully
- New bank information is added or existing bank information is changed on an account shortly after it is opened, particularly when followed by a redemption request

- A report of all accounts that had newly established ACH or bank account information added
- A report of any prepaid debit cards or Green Dot banks added to an account as the bank of record
  - A bank account consisting of 16 digits or longer may indicate that it is associated with a prepaid debit card.
  - The following ABA numbers are currently tied to a Green Dot bank:
    - 0611 2000 0
    - 0960 1741 8
    - 1240 8502 4
    - 1243 0252 9
    - 1243 0132 0
    - 1243 0316 2 (associated with GoBank)
    - 1243 0312 0
    - 0739 7218 1 (associated with MetaBank)

Nonfinancial Transactions

- Multiple contact points (e.g., telephone, email, web, VRU, webchat) occurring on an account within a short period of time
  - Note: multiple contact points could be via the same channel (e.g., telephone) or across various channels (e.g., telephone, web, VRU).
- Multiple recent account changes (e.g., website user ID/password, telephone number, address, email address, addition or change of bank information) within a specified time frame
- A report of accounts that had check writing added for the first time
- A report of accounts that had a change of address to a foreign address
- A report of accounts that had a change of address to a suspected business address
- Suspicious or unusual email names/addresses/domains associated with an account; examples of unusual email domain names include (but are not limited to):
  - @mail.com
  - @homeemail.com
  - @artlover.com
  - @uymail.com
  - @reggaefan.com
  - @acdcfan.com
  - @yandex.com
  - @yopmail.com
  - @opayq.com

- @vfemail.net
- @guerrillamail.net
- @guerillamail.biz
- @guerillamail.com
- @temp-mail.org
- @wiseyoho.com
- @babatfirst.com
- @myyou.com

Examples of unusual email usernames include:

- Username begins with "doctor" plus 4 numbers (e.g., doctor8877@, doctor7878@).
- Username contains a variation of USSERVICE (e.g., usservice@, usservicenow@, usservice101@).

- A phone number, fax number, bank account number, email address, or IP address previously associated with a fraudulent attempt or transaction is added to or associated with an account
- A report of all webchat activity (to review for red flags)

General Review

- An enhanced monitoring[37] report of any account that has been the subject of previous fraud attempts, or whose shareholder has reported that they have been the victim of identity theft, or the account has elements (e.g., phone number) associated with previous fraud attempts

Indicators of Potential Financial Exploitation of Elders or Other Vulnerable Persons

Several recent studies highlight the increase in fraud cases and complaints involving seniors and are helping bring awareness to this growing problem.[38] Unfortunately, though awareness of this significant issue is increasing, incidents of fraud and elder exploitation continue to rise. Funds and transfer agents play a critical role in identifying and reporting senior financial exploitation. To protect elderly investors as well as vulnerable persons,[39] funds and transfer agents could consider the following red flags that may be indicative of financial exploitation.[40]

---

[37] Enhanced monitoring may consist of a review of transactions, maintenances, and web activity as well as telephone interactions.

[38] Examples of recent studies and reports include: *Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors*, available at http://dhhs.ne.gov/Medicaid%20SUA/US%20Senate%20Special%20committee%20on%20Aging%20Fraud%20Book.pdf; *Protecting Older Consumers 2018–2019: A Report of the Federal Trade Commission*, available at www.ftc.gov/reports/protecting-older-consumers-2018-2019-report-federal-trade-commission; "FinCEN Analysis: Bank Secrecy Act Reports Filed by Financial Institutions Help Protect Elders from Fraud and Theft of Their Assets," available at www.fincen.gov/news/news-releases/fincen-analysis-bank-secrecy-act-reports-filed-financial-institutions-help.

[39] The SEC and FINRA define *elder* and *vulnerable* adults as customers who are aged 65 and older as well as those who are aged 18 or older and who, the financial institution reasonably believes, have a mental or physical impairment that prevents them from protecting their own interests. Individual states may have slightly different definitions for who is considered an elder investor (e.g., age 60 versus 65).

[40] Funds/transfer agents may also see these red flags related to accounts associated with the conservatorship or guardianship of a minor or any other vulnerable person.

What to Listen For

Voice

- The caller's voice does not match the age or gender of a senior customer.
- The caller has a foreign accent, which is inconsistent with account information on file.
- The caller uses phrases such as "I've had a tracheotomy," "I've got a bad cold today," or "I just got out of the hospital" as an explanation for age or gender discrepancy when asked further identifying questions.
- The caller's voice sounds electronically modified or monotone with unnatural pauses.
- The caller uses a relay service for the hearing-impaired to request telephone transactions.

Mannerism

- The caller sounds nervous, is evasive, acts confused, or is unable to provide sufficient information to pass the security check.
- The caller sounds coached (or the phone representative can hear someone in the background coaching the caller or directing the shareholder on what to say or what to request).
- The caller seems confused or not fully aware about what he or she is requesting.
- The caller exhibits an extreme sense of urgency or anxiety about the request.
- The caller expresses excitement over a financial windfall or prize check or uses key phrases associated with common exploitation schemes (e.g., sweepstakes, lottery, real estate, home improvement).
- The caller expresses fear or anxiety over an urgent call or notice purportedly from the Internal Revenue Service, Social Security Administration, law enforcement, or an individual demanding financial compensation for a family member in dire straits (e.g., in jail, kidnapped).
- The caller appears to have difficulty speaking or communicating clearly.

What to Look For: General Behavior

- The shareholder wants the phone representative to speak to someone else regarding his or her account.
- The caller lacks knowledge about the type of account, value, or recent activity.
- The caller appears unable to process simple concepts or requests.
- The caller exhibits signs of memory loss.
- The caller's behavior is erratic.
- The caller contacts the call center multiple times (in one day or over a short period of time) with questions regarding processing requirements, account rules, redemption maximums, MSG requirements, or how to add new bank account information to an account.
- The caller cannot be contacted for necessary follow-up or confirmation of activity.
- The caller shows no concern regarding the consequences of financial decisions, including penalties or fees.
- The caller appears to be concerned or confused about missing funds in his/her account, where reviews indicate there were no unauthorized money movements or no money movements at all.
- The customer is not aware of, does not understand, or does not remember recently completed financial transactions.

What to Look For: Account History

- A noticeable change in the shareholder's financial transactions (e.g., more frequent or larger redemptions, which would be inappropriate or out of character for an elderly shareholder)
- Suspicious signatures on checks, service option forms, and other documents when compared against previously received communications (e.g., account application, check writing, or redemption requests); for example, the signature appears to be that of a person younger than the shareholder holding the account
- Multiple or persistent requests to send redemption proceeds to a third party rather than the address of record or bank on file without the proper documentation or required MSG
- A recent addition or change of a POA or other authorized party on an account
- Multiple requests to update a POA, joint owner, or beneficiary information on the account
- A POA who adds themselves as an IRA beneficiary or TOD beneficiary
- Repeated address changes over a short period of time
- A request to change the frequency or increase the amount of an established, ongoing required minimum distribution transaction
- Atypical or unexplained redemptions from the shareholder's account that are outside the norm for the customer

Financial Exploitation or Diminished Capacity

In addition to the above-listed general red flags, there are other signs of elder financial exploitation that fall into three main categories, outlined below.

Confusion or Impaired Cognition Shown by the Shareholder

- An elderly shareholder who cannot easily pass a security check and needs coaching to do so
- An elderly shareholder who lacks knowledge about his or her investment or financial status, cannot explain recent transactions, and/or shows a reluctance to discuss transactions or financial matters
- An elderly shareholder who is confused about the account balance or transactions, legal documents such as POA, and/or their account ownership or registration
- An elderly shareholder's account that has a history of lost or unpaid checks, purchase checks returned for insufficient funds, or repeated orders for a check-writing checkbook
- Drastic shifts in investment style to a higher risk portfolio
- Repeated changes in beneficiaries
- Reluctance to speak when a third party is on the phone
- Providing POA to someone who appears inappropriate

Control and Isolation by a Third Party or Relative of Shareholder

- An elderly shareholder who is assisted by a person, such as a caretaker, relative, or friend, and that person appears to be directing account activity without proper legal documentation
- A sudden or frequent change in an elderly shareholder's financial activity, including a change of POA
- A POA document, especially a springing power of attorney,[41] signed and dated shortly before receiving any request from the designated POA
- A third party assisting the elderly shareholder who shows an excessive amount of interest in the elderly shareholder's investments and assets
- A third party assisting an elderly shareholder who does not allow the shareholder to speak for himself or herself
- Inability to speak directly with the elderly shareholder, despite repeated attempts to contact him or her
- An elderly shareholder who expresses fear or submissiveness toward the POA or third party assisting him or her

[41] A springing power of attorney is a POA document that allows an attorney-in-fact to act for an individual if they become incapacitated; it is not in effect until they are incapacitated. It "springs" into action if they become incapacitated.

Unusual Transactions That Do Not Make Sense

- An attempt by a guardian, conservator, POA, or other third party to transfer assets from an elderly shareholder into his or her name or to another third party
- Unusual requests to change account options, including services that may not be understood by (or be appropriate for) an elderly shareholder; for example:
  - Establishment of online access when none existed previously
  - Change of document delivery methods to e-delivery
  - Addition or change of bank information on file
  - Establishment of a new SWP
- Indications that a shareholder (typically an elderly shareholder) may be a victim of a fraudulent lottery or sweepstakes offer, including:
  - A request to process a redemption to pay for fees, taxes, or customs dues associated with a lottery or contest
  - A request to send redemption proceeds to a red flag destination (e.g., Las Vegas; a sweepstakes organization; a foreign country, such as Nigeria, commonly associated with lottery scams)
  - A reference to wiring money to pay someone claiming to represent a contest or lottery.
  - A reference to needing to pay a fee to receive lottery or contest "winnings"
  - Use of a counterfeit or bad check representing alleged lottery winnings to purchase shares
  - Receipt of a written transaction or maintenance request that includes documents that appear to originate from a lottery scam
- Indication that a shareholder (typically an elderly shareholder) may be the victim of a romance scam, including:
  - Reference to a significant other who they have not met in person or to a new significant other who is in the military, working on an oil rig or pipeline, a doctor for an international organization, or other career that requires extended travel or residence outside the United States
  - An urgent request for a redemption to assist a significant other with a personal emergency or other urgent matter such as needing to purchase a plane ticket, pay off medical expenses or gambling debts, or cover US customs fees or visa charges
  - Reference to a redemption request being made to cover travel expenses to meet their significant other in another state or country
  - A request to wire redemption proceeds to a new significant other in a foreign country

Red Flags in Combination May Indicate a Higher Potential of Fraud

Any of the red flags included in the Indicators of Potential Financial Exploitation of Elders or Other Vulnerable Persons section (see page 26) are by themselves an indication of potential fraud or fraudulent activity. Any combinations of these red flags indicate an elevated fraud potential related to the account and warrant further investigation.

General Fraud Prevention/Red Flag Program Considerations

As funds/transfer agents consider the red flags outlined within this document for inclusion in their training, fraud prevention, and Reg S-ID: Identity Theft Red Flag programs, they may also consider the following:

- Development of a risk-ranking matrix, including the makeup of the fund's shareholder base, products offered by the fund complex, and how the red flag would most likely be detected (e.g., manually or in an automated fashion). Funds/TAs may consider risk ranking various red flags or red flags occurring in combination as being more indicative of fraud or fraudulent activity as appropriate for their organization and shareholder base.
- Development of red flag training programs, including determination of frequency/schedule of training for frontline associates (e.g., annually, semiannually, hot topic specific), format (e.g., classroom versus web-based), and content (e.g., use of live examples from past events to illustrate red flags present or missed). Funds/TAs may also consider identifying skill sets that may assist associates in identifying fraud and developing programs designed to help associates improve upon those competencies.
- Development and communication of escalation protocols, including when to escalate, to whom to escalate (e.g., manager, fraud team, compliance), manner of escalation (e.g., via email, a specific hotline, web portal, phone call), and what facts or information to include. Escalation protocols should be clearly documented and communicated to all associates as appropriate.
- Periodic review to ensure red flags outlined and monitored for are still appropriate, including frequency of review, who is responsible for the review, what is to be reviewed, and protocols for change.
- Continuous improvement—evaluating and finding solutions to:
  - identify red flags across communication channels (e.g., telephone, web, email) affecting the same shareholder or account;
  - track multiple telephone calls to different call center representatives from a single caller inquiring about the same account; and
  - shift back-end controls into real time using new and emerging technologies.

INVESTMENT COMPANY INSTITUTE®

WASHINGTON, DC • LONDON • HONG KONG • WWW.ICI.ORG