

# Western & Southern Financial Group Anti-Fraud, Elder Abuse & Financial Exploitation Training (2023)



For Gerber Life associates.

Action Required: Carefully read the training information, complete the quiz with at least an 80% and acknowledge receipt of the training information.

☰ What is Insurance Fraud?

☰ Preventing and Detecting Insurance Fraud

☰ Elder Abuse & Financial Exploitation

☐ ? Anti-Fraud, Elder Abuse & Financial Exploitation Training Quiz

☰ Course Complete

# What is Insurance Fraud?

---



## Fraud within the Industry

Fraud can be emotionally and financially devastating for all parties involved:

- According to the FBI, insurance fraud (non-health insurance) costs the economy over \$40 billion each year.<sup>1</sup>
- Insurance fraud steals at least \$308.6 billion every year from American consumers.<sup>2</sup>
- Insurance fraud (non-health insurance) costs the average U.S. family between \$400 and \$700 per year in the form of increased premiums.<sup>1</sup>



<sup>1</sup> This statistic includes life insurance as well as property and casualty insurance. <https://www.fbi.gov/stats-services/publications/insurance-fraud>

<sup>2</sup> <https://insurancefraud.org/fraud-stats/#:~:text=Insurance%20fraud%20steals%20at%20least,of%20property%2Dcasualty%20insurance%20losses.&text=The%20FBI%20estimates%20non%2Dmedical,least%20%2440%20billion%20every%20year>

## What is Insurance Fraud?

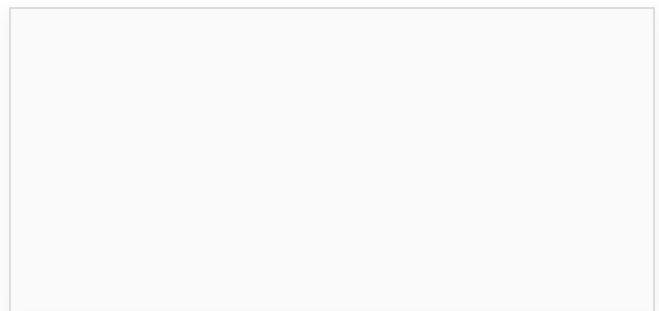
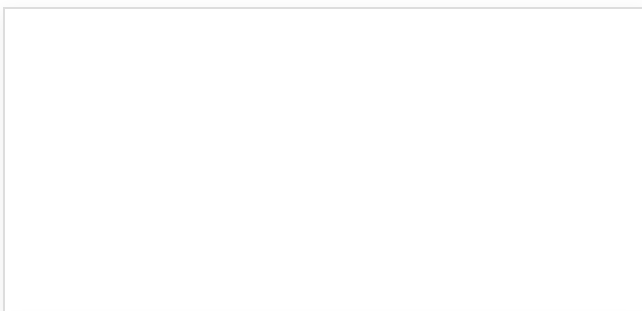
Insurance fraud occurs when people deceive an insurance company to receive compensation or other benefits to which they are not entitled.

Like other forms of fraud, insurance fraud requires the perpetrator to knowingly make a false or misleading statement.

## When Does Insurance Fraud Occur?

Insurance fraud can occur any time during a policy or contract's lifetime, including, but not limited to:

[Click each card to reveal the answers]





During the underwriting process



In connection with a claim or application for other benefits



Through a third-party  
account takeover

## Who Can Commit Insurance Fraud?

Insurance fraud can be committed by any individual involved in a transaction, including, but not limited to:

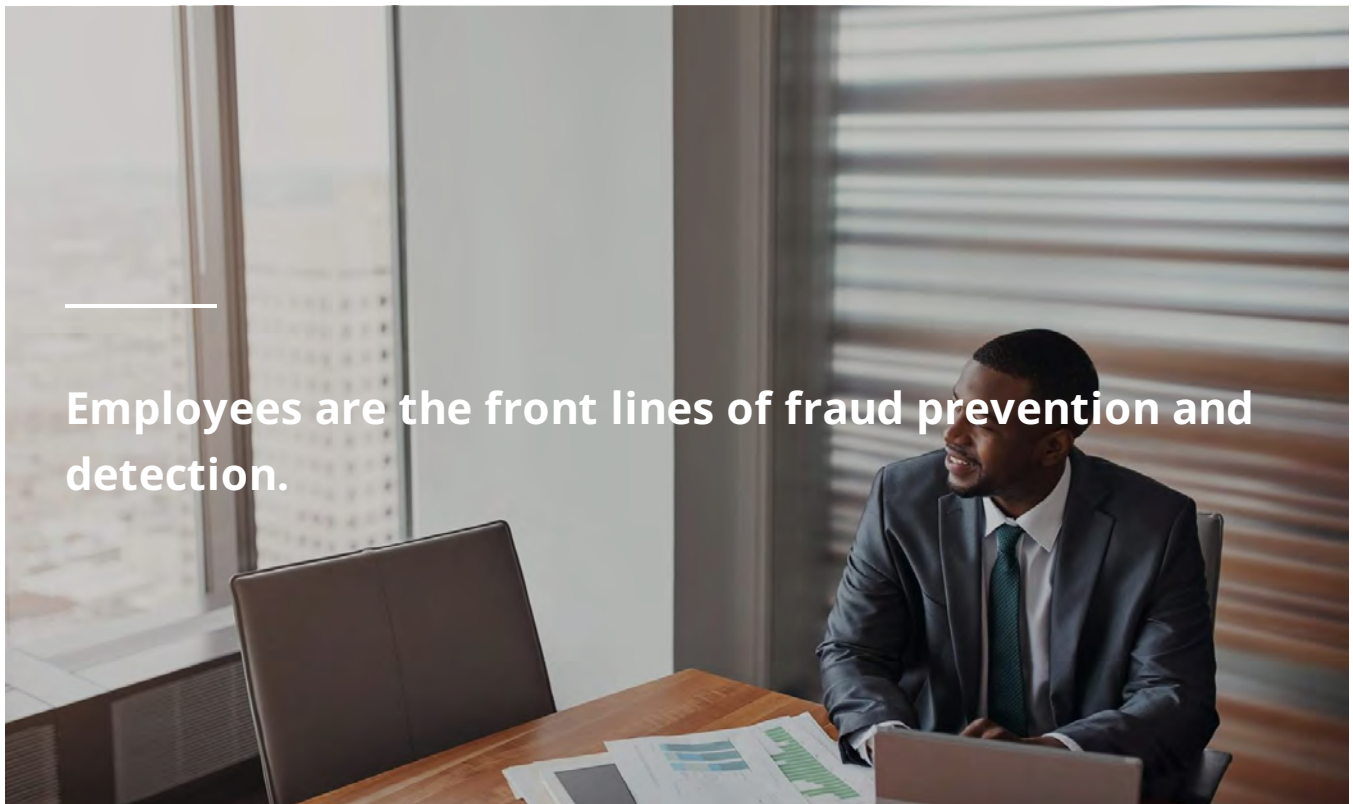
- Policy or contract owners;
- Beneficiaries;
- Insurance agents;
- Insurance company employees; and
- Other third-parties, e.g., criminals.



Complete the content above before moving on.

# Preventing and Detecting Insurance Fraud

---



Employees are the front lines of fraud prevention and detection.

Every Western & Southern Financial Group employee has a responsibility to prevent and detect fraudulent activities by identifying and reporting suspicious activities.

To be able to identify suspicious activities, it is necessary to know the potential red flags of insurance fraud.

## Red Flags – Underwriting Process

Red flags during the underwriting process include, but are not limited to:

- Applicant/caller does not know information like a DOB, address, etc.;
- Information on the application is vague or ambiguous as to details of health history, dates, places of treatment, names of physicians or hospitals, etc.;
- Application for insurance is for an amount of insurance just under the threshold for a full evaluation of health (e.g., blood or paramed);
- Names and other important information are spelled wrong;
- Applicant fails to sign and date the application;
- Pertinent questions are not answered on the application (e.g., income, other insurance, hazardous duties or activities, etc.);
- Applicant has a history of many insurance claims and losses;
- Information on the application is inconsistent with prior applications;
- Documents are altered;
- Signatures are inconsistent;
- Information is inconsistent with publicly available information;
- Physician's report is vague on details of medical history or inconsistent with the information shown on the application; and
- Applicant has unclear sources of income.

## CONTINUE TO KNOWLEDGE CHECK

Red flag(s) for fraud that can be identified during the underwriting process is/are: (select all that apply)

---

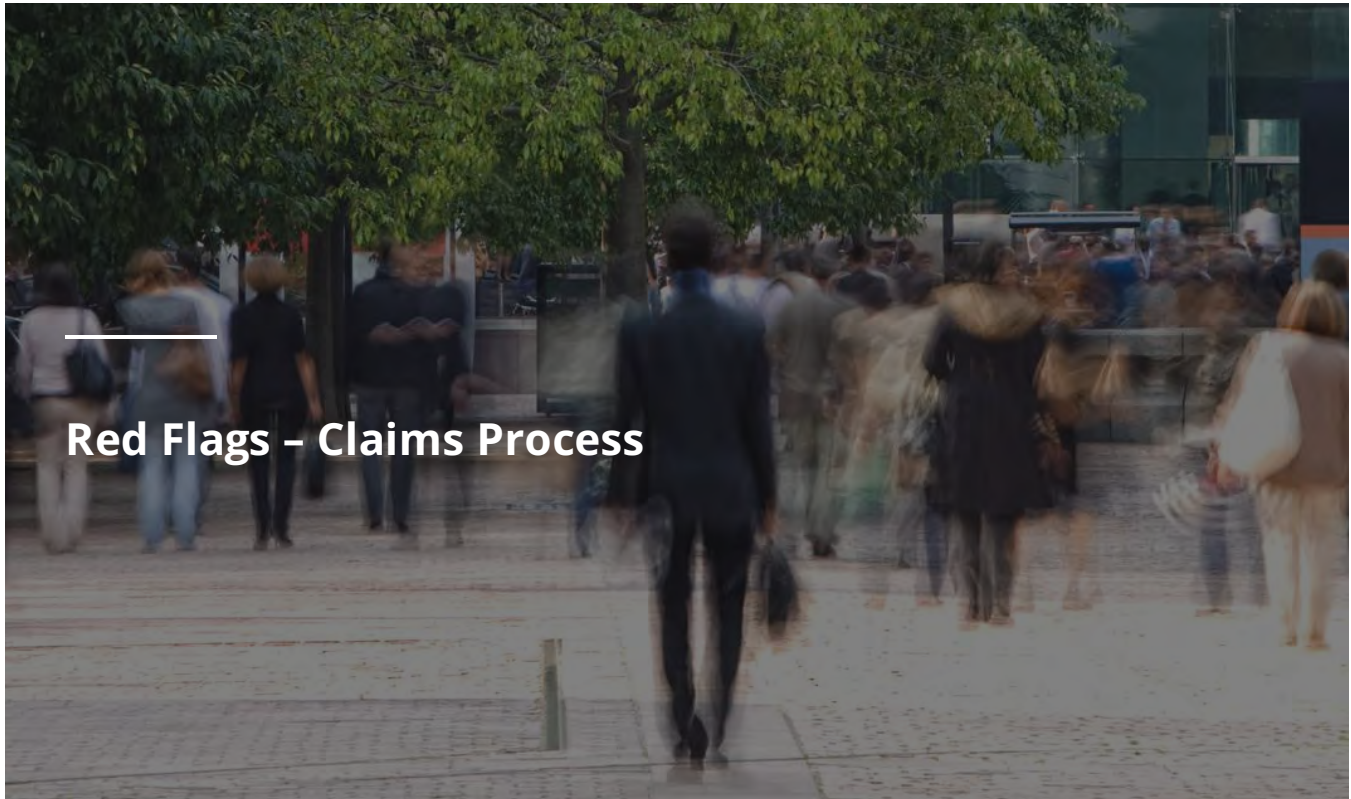
- Names are spelled wrong
- Information is consistent with other information on file for the applicant
- Physician's report is vague on details of past medical history
- Application for insurance is for an amount of insurance just under the threshold for a full evaluation of health (e.g., blood or paramed)

SUBMIT





Complete the Knowledge Check before moving on.



Red flags during the claims process which may indicate potential fraud include, but are not limited to:

- Claimant is missing necessary identifying information (e.g., DOB, address, account information, etc.);
- Names and other important information on a claim are misspelled;
- The information on a claim is inconsistent with the information on file or on the application;

- Documents are altered;
- Signatures are inconsistent on forms;
- Claimant attempts to demand unreasonable processing timetable;
- Long delay between the date of death and submission of a claim;
- Forms of proof of death are suspicious or incomplete;
- Death occurred in a foreign country or the beneficiary lives in a foreign country;
- Disappearance of the insured where no body has been recovered and/or no evidence of death exists;
- Over-submission of documentation, including submission of information not requested;
- Beneficiary information, including contact information, is vague or incomplete;
- Last change of beneficiary was completed by an attorney-in-fact who named themselves as beneficiary; and
- Change of beneficiary dated shortly before the death of the insured.

**CONTINUE TO KNOWLEDGE CHECK**

Which of the following is not a red flag for claim fraud?

- Death occurred in a foreign country or the beneficiary lives in a foreign country
- Forms of proof of death are incomplete
- Over-submission of documentation, including submission of information not requested
- Premium payments are submitted on an agent's personal check

SUBMIT



Complete the Knowledge Check before moving on.

## Red Flags – Surrender, Loan or Withdrawal Process

Red flags during the surrender, loan or withdrawal process which may indicate potential fraud include, but are not limited to:

- Agent requesting surrender checks be sent to him / her for delivery;

- Purported requests by owner to send surrender check to address other than listed on policy or contract;
- Signatures that do not match those in file;
- Altered documents;
- Attorney-in-fact makes request, and file shows owner is handling all transactions prior to surrender;
- Owner volunteers reason for surrender that doesn't seem reasonable;
- Request from owner or agent to not divulge surrender to anyone;
- Caller ID is blocked; and
- Electronic fund transfer (EFT) information cannot be validated.

Red flags for account takeovers are often identified during the surrender, loan, or withdrawal process. Account takeover is a form of fraud involving an unknown third party gaining access to unique details of a customer's account. The fraudster will pose as the real customer and gain access to make changes to the real customer's account, withdraw funds, surrender the policy, request a loan, or obtain other identifying information of the customer.

## **Red Flags – Account Takeovers**

Account takeovers can involve a client's identity, an agent's identity, a policy/contract, or a benefit or pension account. These red flags include, but are not limited to:

- A caller has trouble answering customer/agent authentication questions like date of birth, agent number, SSN, etc.;

- A caller answers customer/agent authentication questions incorrectly, but with a confident tone;
- The caller's voice doesn't fit the customer/agent;
- Documentation appears altered;
- Signatures on information received from the policy/contract owner do not match the policy/contract owner's signatures on applications or other documents;
- A caller seems to be fishing for information; and
- The person trying to complete a transaction is overly persistent or aggressive when following up.

**CONTINUE TO KNOWLEDGE CHECK**

A caller having trouble answering certain customer authentication questions like date of birth, SSN, etc. would typically be an example of a red flag for:

- 
- An Account Takeover
  - Forgery
  - Agent Fraud

None of the Above

SUBMIT

Which red flag(s) could be identified during the surrender, loan or withdrawal process? (select all that apply)

---

A loan request is made by the client's attorney-in-fact

Agent requests surrender checks to be sent to him/her for delivery

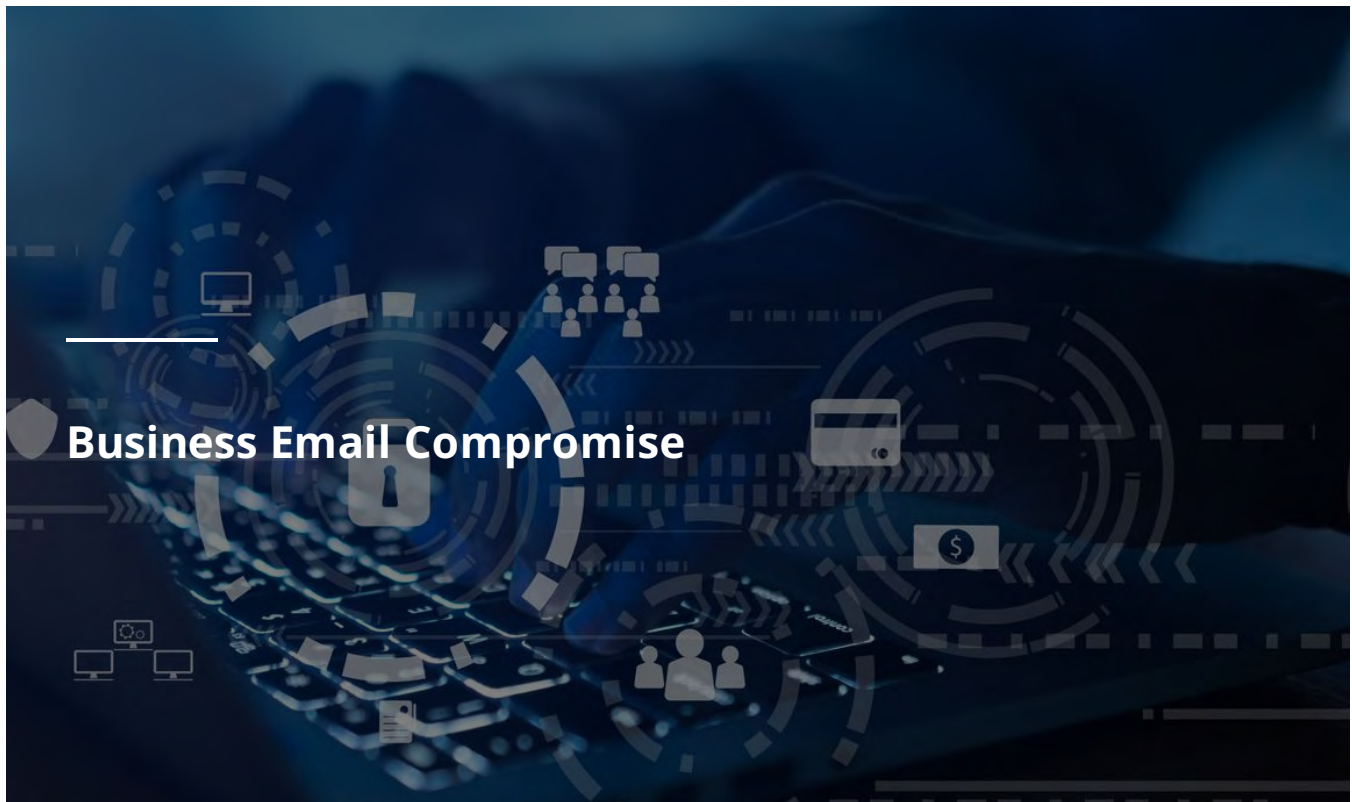
EFT information cannot be validated

Documents appear altered

SUBMIT



Complete the Knowledge Check before moving on.



Another fraudulent scheme, involving an account which has been taken over, is business email compromise (BEC). BEC is becoming an increasingly common way for fraudsters to attack insurance companies. It occurs when a legitimate email account is compromised and used to attempt fraudulent acts. According to the FBI's 2021 Internet Crime Report, BEC scams made up \$2.4 billion of the \$6.9 billion lost to online scams reported to the FBI.<sup>3</sup> Producers and third party vendors our company does business with are the most at risk for BEC.

 <sup>3</sup> [https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)

The following path is a common BEC scenario:

- First, fraudsters gain access to a third party's email account.
- Then fraudsters monitor email activity searching for any emails detailing transfers of money. They look for things like withdrawal/loan/surrender forms, invoices, etc.
- At the most opportune time, the fraudsters insert themselves into a transaction to divert the funds. This can be accomplished by intercepting, altering any of the forms mentioned above, and sending them back to the insurance company for processing. Fraudsters may also email the company directly, acting as the third party, and requesting a fraudulent transaction.
- Because the transaction appears to be legitimately requested by a trusted third party, the fraudulent transaction is more likely to be processed.

Some key items to keep in mind regarding BEC are:

- Always carefully review instructions from clients, producers or vendors that come via email to ensure they are legitimate requests.
- Carefully review the email addresses in emails you receive for email spoofing which is sometimes used in conjunction with BEC. A spoofed email is sometimes used to impersonate another party to the transaction when the fraudster has only compromised one party's email address via BEC. A spoofed email address closely resembles the correct one, but differs slightly, for example:



- Correct email address: joe.smith@westernsouthernlife.com
- BEC email address: joe.smith@westemmsouthernlife.com
- When in doubt, reach out to the person the email purportedly came from (in a different manner than email) to confirm the transaction.

Additional red flags of BEC include:

- A bank account change coupled with a disbursement request (same or separate emails);
- Rush or priority request(s);
- Change in established payment method (e.g. from EFT to check);
- Excessive follow-up to ensure a change / transaction is processed;
- Change in client or vendor's typical communication style (may include misspellings, or just how they write);
- The sender's email address (and possibly other contact information) changes at some point during the "conversation";
- An atypical request, which does not follow a client's past behavior (e.g. timing, size of transaction requests, etc.);
- Transfer instructions refer to a bank located in a different state, region, etc. from account owner; and
- Attempting to bypass typical communication or validation methods (e.g. requesting forms delivered via email rather than mail or attempting to avoid phone calls).

## CONTINUE TO KNOWLEDGE CHECK

Which of the following is/are red flag(s) for BEC? (select all that apply)

---

- Excessive follow-up to ensure a change/transaction is processed
- Change in established payment method
- Client requests for funds from a loan request be directly deposited into their bank account
- A rush request

SUBMIT



Complete the Knowledge Check before moving on.

## Red Flags – Agent/Employee Fraud

An insurance agent or insurance company employee may also be involved in fraud. Red flags involving an agent or employee which may indicate potential fraud include, but are not limited to:

- Premiums submitted on an agent's personal or agency check;
- Agent listed as owner, contingent owner, annuitant, beneficiary, assignee, guardian, or attorney-in-fact;
- Requests for surrender checks to be mailed directly to an agent for delivery;
- Employee or agent demands that others in the company not contact a customer;
- Employee or agent requests for multiple or repeated exceptions to a standard process.

[CONTINUE TO KNOWLEDGE CHECK](#)

Which is/are red flag(s) for agent/employee fraud? (select all that apply)

Employee/Agent requests for multiple exceptions to a standard process

Premium payments submitted on an agent's personal check

Agent is listed as a client's attorney-in-fact

A request for a surrender check to be mailed to the agent

SUBMIT



Complete the Knowledge Check before moving on.

## Preventing and Detecting Insurance Fraud

To help prevent and detect fraud, it is important to fully verify the identity of individuals (including customers and agents) prior to communicating with them. Nonpublic information, including customer, agent, and policy/contract information, should only be provided to individuals who are authorized to receive it.



Do not provide any nonpublic information to an individual who is not able to provide the necessary information to verify their identity. If an individual is unable to provide the necessary information to verify their identity and other red flags indicating potential fraud arise through the verification process, notify your manager for possible additional investigation.

- A red flag does not necessarily mean that fraud has occurred, but it is an indicator of potentially fraudulent activity which may require additional investigation.
- If you identify red flags indicating potential fraud, escalate the potentially fraudulent activity to your manager.
- Remember, if something appears to be potentially fraudulent, or doesn't seem right, ask questions and escalate the potentially fraudulent activity to your manager.

## CONTINUE

### **Special Investigative Unit (SIU Committee)**

Associates are required to follow suspected fraud procedures and notify their managers when they suspect fraud. Managers are required to report all cases of suspected fraud to the SIU Committee. The SIU Committee is responsible for reviewing, investigating, reporting, and taking appropriate actions with respect to suspected fraudulent insurance acts. It is important that all suspected fraud be reported to the SIU Committee to ensure a proper investigation is conducted and all required reporting obligations are met.

#### **Attention Gerber Life Associates**

Gerber Life has an established Fraud Prevention Plan that is located in the Knowledge Hub and N:\\_Public\SIU\Fraud Prevention Plan SOP (4800-LG-SOP-025 v 2). This Fraud Prevention Plan establishes Gerber Life's Special Investigative Unit (SIU) to investigate suspected insurance fraud.

#### **Referral Process for Suspected Fraud**

If fraud is suspected, discuss the situation with your Supervisor or Manager. If your Supervisor or Manager agrees that the activity is suspicious, complete a Suspected Insurance Fraud Referral Form, located in the Gerber Life Knowledge Hub System and at N:\\_Public\SIU\Suspected Insurance Fraud Referral Form and email it to [USNINglic-QACompliance@gerberlife.com](mailto:USNINglic-QACompliance@gerberlife.com).

Your SIU department member and the Legal Department stand ready to assist in the consideration as to whether an activity is suspicious.

### **Gerber Life Contact Center Referral Process for Suspected Fraud**

In the Contact Center, warm transfer the call to QCT. If warranted, QCT will provide the completed Suspected Insurance Fraud Referral Form to Gerber Life's Legal Department.

### **Referral Process for Independent Producers suspecting fraud on a Gerber Life policy**

If fraud is believed to have occurred or is occurring, complete a SIU Referral Form from the Agent Portal and email it to [USNINglic-QACompliance@gerberlife.com](mailto:USNINglic-QACompliance@gerberlife.com).

Additional Questions: 231-928-3688



Complete the content above before moving on.

# Elder Abuse & Financial Exploitation

---



## **Background: Elder Abuse**

Elder abuse has become an increasing concern in recent years. According to the National Council on Aging, 1 in 10 Americans over the age of 60 have experienced some form of elder abuse.<sup>4</sup>

All 50 states have laws protecting those who report elder abuse from civil and criminal liability, provided the report is made in good faith. In addition, many states have laws that mandate specified persons report elder abuse. This means that if a person knows of potential abuse they must report the abuse, or be subject to potential criminal and/or civil penalties.

Federal Law provides a safe harbor for firms to freeze distributions from a client's securities account for a limited period of time to allow the firm to determine if financial exploitation may be occurring and take measures to prevent or mitigate it.



Detecting and reporting elder abuse is EVERYONE'S RESPONSIBILITY!

 <sup>4</sup> <https://www.ncoa.org/public-policy-action/elder-justice/elder-abuse-facts/>

## What is Elder Abuse?

Elder abuse is an intentional act or failure to act by a caregiver or other person in a relationship involving trust that causes or creates a risk of harm to an older adult.

Regulations differ regarding persons covered by elder abuse regulations. For the purposes of our internal policies and procedures, covered persons include anyone over the age of 60 or anyone with an intellectual disability that would make them particularly vulnerable to abuse.

[Drag the examples below to the correct box to indicate whether they are covered or not covered]

Covered

A 61 year-old man

An 18 year-old with  
intellectual disability

A 50 year-old woman with  
early onset Alzheimer's  
disease

Not Covered

## Types of Elder Abuse

There are many types of elder abuse, including:

[Click each card to reveal the definitions]

Physical Abuse

Use of physical force or  
inflicting pain or injury upon  
a person.

---

## Self Neglect

A term used to describe a vulnerable adult living in a way that puts his or her health, safety, or well-being at risk. Although it doesn't involve a third party perpetrator, it is still considered a form of elder abuse.

---

## Neglect by Others

Occurs when a caretaker fails to provide the goods and services required to prevent physical harm, mental suffering or illness.

---

Abandonment

Desertion of a senior that  
relies on a person for care.

---

Emotional Abuse

Use of threats, humiliation,  
or intimidation to cause  
psychological harm to a  
senior.

Sexual Abuse

Non-consensual sexual activity with a senior or vulnerable adult.

Financial Exploitation

Occurs when a person illegally or improperly uses a protected adult's funds or assets for the profit or advantage of someone other than the protected adult. This can happen through fraud, theft, conspiracy, deception, threat, or intimidation.

[CONTINUE TO KNOWLEDGE CHECK](#)

In terms of elder abuse, an example of a covered person is:

- A 55 year-old woman
- A 25 year-old woman with a cognitive handicap
- A 50 year-old man
- An 18 year-old man with a physical handicap

SUBMIT



Complete the content above before moving on.

A background image featuring various financial charts, including line graphs and candlestick patterns, overlaid on a dark blue grid. The charts show different trends and data points, with some labels like '183 + 5.10%' and '102 + 7.51%'.

**What is Financial Exploitation?**



Financial exploitation has been defined as the wrongful or unauthorized taking, withholding, appropriation, or use of a specified adult's funds or Securities.

It also includes any act or omission taken by a person to deprive a specified adult of his or her ownership, use, benefit, or possession of his or her money, assets, or property through:

- Improper use of a power of attorney, guardianship, or conservatorship;
- Obtaining control through deception, intimidation, or undue influence; or
- Converting the money, assets, or property of such an individual for personal financial gain.

The National Council on Aging estimates that financial exploitation and fraud cost older Americans \$2.9 billion to \$36.5 billion a year.<sup>5</sup> Due to its increasing prevalence, many states have specific regulations regarding financial exploitation.

 <sup>5</sup> <https://www.ncoa.org/public-policy-action/elder-justice/elder-abuse-facts/>

Financial exploitation can take many forms such as:

[Please click each item below to learn more]

## **Theft** —

Theft is the action of stealing or misappropriation of a vulnerable adult's income or assets. Examples of theft include:

- unauthorized withdrawals from a vulnerable adult's account;
- forging checks or legal documents; and
- using ATM or credit cards without permission.

## **Coercion/Undue Influence** —

Coercion/Undue Influence is the practice of persuading someone to do something by using force or threats. Examples include:

- withholding care in an effort to be granted access to funds;
- emotional intimidation; and
- withholding information or lying in an attempt to gain access to assets.

## **Abuse of Legal Authority** —

Seniors or other vulnerable adults may grant legal authority, such as power of attorney or guardianship, to another individual to help manage finances and make decisions on their behalf.

Abuse of this authority means that the appointed individual uses their legal authority to steal or misappropriate the vulnerable adult's funds or assets for personal use.



## Scams —

Scams are dishonest schemes. Examples of scams that may affect vulnerable adults include:

- sweetheart scams;
- false charity scams;
- grandparent scams;
- false lottery or sweepstakes scams;
- home repair scams;
- email and telemarketing scams; and
- Medicare/Medicaid fraud.

[CONTINUE TO KNOWLEDGE CHECK](#)

Which of the following is not a method of financial exploitation?

- 
- Theft
  - Helping an elderly person pay their bills
  - Coercion
  - Abuse of legal authority

SUBMIT



Complete the content above before moving on.

## Potential Perpetrators

Most instances of elder abuse or financial exploitation are perpetrated by family members. Other potential perpetrators include:

- Friends;
- Acquaintances;
- Romantic partners;
- Professional caregivers;
- Healthcare providers; and
- Third parties engaged in fraud or scams.

## Red Flags of Elder Abuse and Financial Exploitation

Red Flags for Elder Abuse Include:

- Large or uncharacteristic gifts or loans.
- Isolation of a vulnerable adult by a caregiver.
- Inability to make decisions.
- Changes in personal hygiene.
- Changes in mood or temperament.
- Bruises or other injuries.
- Unusual changes in bank account or money management.
- Family member or caregiver does not allow the client to speak or is reluctant to leave the client's side during conversations.
- Inability to contact or speak directly with the client despite several attempts.
- Lack of documentation for claimed legal authority.
- Multiple individuals claiming legal authority.
- Frequent changes to account beneficiaries.

Red Flags Specific to Financial Exploitation include:

- Sudden changes in bank accounts.
- Unexplained withdrawals of large amounts of money.

- Abrupt changes in will or other beneficiaries.
- Unpaid bills despite the availability of adequate financial resources.
- Forging of a senior's signature.
- Unexplained transfer of assets to a third party.

[CONTINUE TO KNOWLEDGE CHECK](#)

Which of the following is a not red flag for elder abuse?

---

- Changes in hygiene.
- Large or uncharacteristic withdrawals from an account.
- Undue deference in the presence of a caregiver.
- Providing power of attorney (POA) documentation.

[SUBMIT](#)

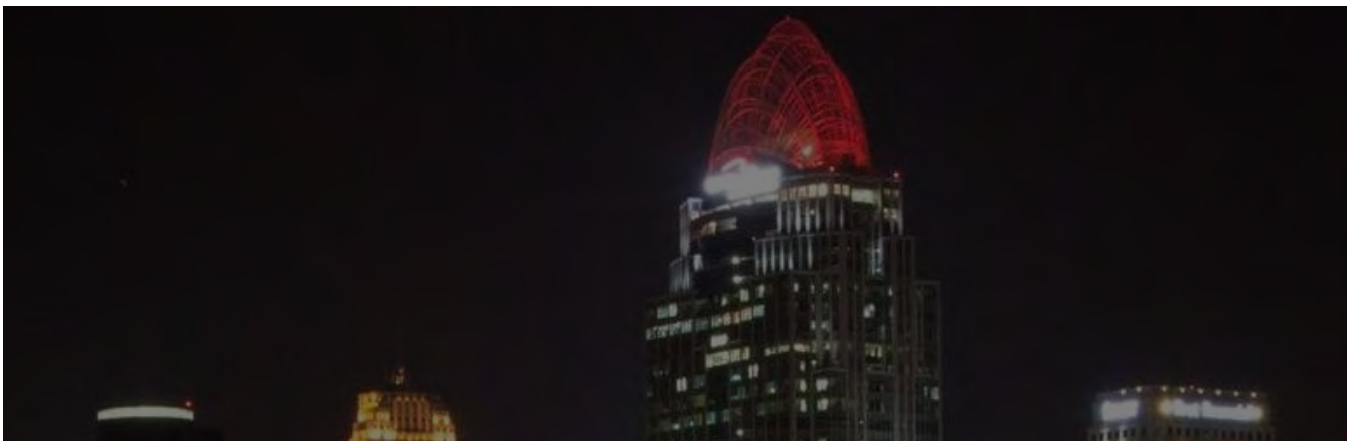



Complete the content above before moving on.

## Who is at Risk?

There are certain risk factors that make some more vulnerable to elder abuse or financial exploitation, including:

- Those with low social support;
- Those who have low income;
- Those in poor health;
- Those who are dependent on others for care or assistance with activities;
- Those suffering from Alzheimer's, dementia or diminished capacity; and
- Those who are non-verbal or have a lack of ability to communicate.





## What To Do If You Suspect Elder Abuse

Associates are required to follow their suspected elder abuse and financial exploitation procedures and notify their managers when they suspect elder abuse or financial exploitation.

Managers are required to report all cases of suspected elder abuse or financial exploitation to the SIU Committee.

The SIU Committee is responsible for reviewing, investigating, reporting, and taking appropriate actions with respect to suspected elder abuse or financial exploitation.

It is important that all suspected elder abuse or financial exploitation be reported to the SIU Committee to ensure a proper investigation is conducted and all required reporting obligations are met.

### **Attention Gerber Life Associates**

Gerber Life has an established Preventing Financial Exploitation SOP that is located at n:\\_Public\SIU\Financial Exploitation SOP. This Preventing Financial Exploitation SOP sets forth Gerber Life's

program to prevent and detect the Financial Exploitation of its customers.

### **Referral Process for Suspected Financial Exploitation of a Vulnerable Adult**

If financial exploitation or fraud is suspected, discuss the situation with your Supervisor or Manager. If your Supervisor or Manager agrees that the activity is suspicious, complete a Suspected Insurance Fraud Referral Form, located in the Gerber Life Knowledge Hub System and email it to [USNINglic-QACompliance@gerberlife.com](mailto:USNINglic-QACompliance@gerberlife.com).

Your SIU department member and the Legal Department stand ready to assist in the consideration as to whether an activity is suspicious.

### **Gerber Life Contact Center Referral Process for Suspected Financial Exploitation of a Vulnerable Adult**

In the Contact Center, warm transfer the call to QCT. If warranted, QCT will provide the completed Suspected Insurance Fraud Referral Form to Gerber Life's Legal Department.

### **Referral Process for Independent Producers suspecting financial exploitation of a vulnerable adult regarding a Gerber Life policy**

If financial exploitation or fraud is believed to have occurred or is occurring, complete a SIU Referral Form from the Agent Portal and email it to [USNINglic-QACompliance@gerberlife.com](mailto:USNINglic-QACompliance@gerberlife.com).

Additional Questions: 231-928-3688

[CONTINUE TO FINAL QUIZ](#)



Lesson 4 of 5

# Anti-Fraud, Elder Abuse & Financial Exploitation Training Quiz

---

*Question*

**01/10**

When can insurance fraud occur? Select all that apply.

---

- During the application process.
- During the underwriting process.
- During the claim process.

Question

02/10

Who is responsible for identifying and reporting elder abuse and financial exploitation?

---

- Senior Management.
- Sales Agents.
- Compliance Associates.
- Everyone.

*Question*

**03/10**

Indications of forgery or an altered document include (select all that apply):

---

- Traces of previous writing
- Appearance of cut lines
- Document signed by an attorney-in-fact
- Absence of printed material that should be present on the form

*Question*

**04/10**

Financial exploitation includes all of the following except:

---

- Improper use of a power of attorney, guardianship, or conservatorship.
- Obtaining control of a person or their assets through deception, intimidation, or undue influence.
- Obtaining guardianship of an elderly family member suffering from dementia.
- Converting the money, assets, or property of an individual for personal financial gain.

*Question*

**05/10**

Please fill in the blank: Insurance fraud (non-health insurance) costs the average U.S. family between (\$) \_\_\_\_\_ per year in the form of increased premiums.

---

- \$100 and \$300
- \$400 and \$700
- \$800 and \$1000
- \$1000 and \$1500

*Question*

**06/10**

True or False: Caregivers and healthcare providers are typically not in a position to commit elder abuse.

---

True

False

*Question*

**07/10**

Please select the correct statement(s):

---

- The discovery of a red flag means that fraud has occurred.
- Insurance fraud is only committed by agents.
- The alteration of documents and the forgery of signatures can occur on any standard company form.
- Fraud cannot be identified during the underwriting process.



*Question*

**08/10**

Red flags of elder abuse or financial exploitation include: (select all that apply)

---

- Inability to make decisions.
- Changes in personal hygiene.
- Submitting power of attorney (POA) documentation.
- Unexplained withdrawals of large amounts of money.
- Appointing a trusted contact when opening an account.
- Abrupt changes in will or other designations.

*Question*

**09/10**

A family member who signs a loan request as a client's attorney-in-fact without the client's knowledge then keeps the money for themselves describes which method of elder abuse?

---

- Physical Abuse
- Abuse of Legal Authority
- A Scam
- Coercion

*Question*

**10/10**

The group that is responsible for reviewing, reporting, and taking appropriate actions to resolve all suspected fraudulent insurance acts is:

---

- The Special Investigative Unit Committee
- The Law Department
- The Anti-Fraud Group
- None of the Above

# Course Complete

---

