New Hire Anti-Money Laundering & Fraud Prevention Training

Presented by the Compliance Department
of Security Benefit Corporation

December 2019

Fraud Prevention Training

Yes, fraud attempts do happen here. How has Security Benefit been affected by fraud?

Security Benefit has been victimized by several incidents of fraudulent withdrawals in the recent past. Following are some of the red flags to look for, as well as information about the costs that can be incurred as a result of accepting and processing these withdrawals.

- Nearly all of the incidents included withdrawal forms being submitted by fax, and many of the fax numbers for these incidents were from area codes that did not correspond to the area codes for the customers' telephone numbers we had on file.
- The withdrawal requests directed that funds be sent electronically, either by wire or by EFT.
- While many of the withdrawals were for very large dollar amounts relative to the values of the contracts, others were for smaller amounts (but still in the thousands of dollars).

Several of the fraudulent withdrawal requests were accompanied by void checks that weren't genuine. One incident in particular is discussed in more detail later in this section (see slide number 7).

Altogether, these withdrawals have cost Security Benefit a significant amount of money to reimburse the impacted customers. The time and effort spent investigating incidents and submitting required state fraud reports was also considerable.

You can be the first line of defense against fraud.

What is fraud?

An intentional act of deception, misrepresentation, or concealment committed in order to gain something of value.

Why is annual anti-fraud training required?

- To raise awareness of fraudulent activity in the insurance services and financial services industries
- To provide up-to-date information regarding new fraud schemes and/or red flags
- To satisfy regulatory requirements

Some states require annual training for those employees who are considered to be “integral anti-fraud personnel” and who are in the position to detect potential fraud.

Why should you be concerned about fraud?

In general, employees of all organizations should be interested in stopping fraud because it might decrease corporate growth and employee opportunities. Fraud loss, if discovered too late, might even tarnish the reputation of an organization and its employees. Ultimately, occupational fraud is costly to society because it negatively affects everyone’s disposable income through reduced stock market prices and higher taxes. Each individual has an ethical responsibility to reduce fraud and its effects.

It is always important to be vigilant for potential fraud and take the proper steps if a suspicious transaction arises, as the losses resulting from fraud can have a significant impact on the bottom line of the company.

What types of fraud could affect Security Benefit and its affiliated companies?

- ❑ Account Takeover
- ❑ Check fraud
- ❑ Churning
- ❑ Claims fraud
- ❑ Identity Theft
- ❑ Internal Fraud
- ❑ Financial Exploitation of Vulnerable Persons



Check Fraud

The company receives scores of checks every day from individuals and businesses. Associates need to be aware of the various methods with which the company could be taken advantage of by accepting fraudulent checks.

1. Altered checks

   Someone takes a legitimate check and uses chemicals or other means to erase the amount or the name of the payee so that new information may be entered. Look for suspicious markings, crossed out writing, or chemical smells on the check.

2. Counterfeit checks

   - May be in one of two forms: one form of counterfeiting is when a check is presented with fraudulent manipulations or due to theft; another form is when a false check is drawn on a valid account.
   - One way to identify a false check is to see if it lacks perforations. Legitimate checks are perforated on at least one edge, i.e., it came out of real check book or ledger and was not produced on plain paper from a printer. You can also look for unusual toner issues to identify checks that were most likely produced on a color copier or printer.
   - Examine the check for any misspelled pre-printed words. Professional checks should not have misspelled words. Check fraud perpetrators are notoriously bad spellers.

3. Forged checks

A forgery occurs when an individual signs another person's name or electronically produces the other person's signature without that person's consent. This can occur on the signature line of a check or on the endorsement appearing on the reverse side of the check. It is important to routinely compare signatures on checks to others in the customer's file to ensure the signature appears legitimate. While some variation in signatures is normal, especially over time, significant variations can be suspicious.

A signature should also be considered suspicious if it appears to be an exact copy of a prior signature on file.

An example of check fraud:

A check used to open an account has $3,600 written in the $ amount box, but "Thirty-six and 00/100" is written on the line below it. The check is deposited in the amount of $3,600, and the customer withdraws $3,600. But the check is only worth $36. The rule for financial institutions is that the written line is the amount used for authentication purposes.

Churning

Churning is the practice of a sales representative engaging aggressively or excessively in trading a customer's account, or inducing an annuity owner to replace the existing contract with one providing lesser benefits primarily to generate commissions rather than to benefit the customer.

Red Flags

- The bulk or even all of financial professional's business is replacement contracts
- An annuity is surrendered during the surrender charge period, the proceeds transferred to another insurer, and then moved back to the first company in a short time frame
- A general power of attorney is given to a financial professional (one with no limitations as to what the attorney-in-fact may sign on behalf of the customer)

An example of churning:

Jane Doe's Security Benefit variable annuity contract is out of surrender charges. Her financial professional, Bob Jones, moves a percentage of these funds to variable annuities Jane holds at other carriers, which creates commissions for Bob. Over time, Bob returns part or all of the funds to the original contract with Security Benefit where he is again paid commissions on the contribution. Bob has now been paid commissions several times on the same money. As a financial professional, Bob should act for the benefit of Jane Doe instead of his own financial interest.

Claims Fraud

Claims fraud can generally be described as a false statement, misrepresentation, or deliberate omission that is critical to the determination of benefits payable or that results in some unauthorized benefit to a claimant or some other party. Claims fraud can also include forgery or alteration of policy related items such as loans, surrenders, assignments, changes in beneficiary, false withdrawal requests, etc.

It is important to follow the proper procedures when processing a death claim in order to ensure all paperwork is received and in good order and no red flags are present.

Red Flags

- Incomplete or altered claim forms
- Signature inconsistencies
- Reluctance to provide death certificate or claim that owner died abroad
- A beneficiary who makes excessive demands for fast payment of the proceeds
- Request to wire transfer a death benefit payout, especially to a foreign account
- Personal information on death certificate differs from that on the application
- New bank account information that has not been confirmed as the client's

Examples of Fraud at Security Benefit

1. A single premium annuity was purchased as part of a settlement. The individual receiving the annuity payout was to receive it for a period certain or death. The annuitant died. The death was not reported to Security Benefit, and the spouse forged documentation that the annuitant was still alive and received fraudulent payments of approximately $500,000. (*Forgery was also a part of this fraud.)

2. SBL received multiple Scheduled Systematic Withdrawal (SSW) requests bearing signatures that had no resemblance to the owner's signature on the application or prior withdrawal forms SBL received. The SSW forms also indicated a telephone number for the owner that was different than the number for the owner in SBL's records (and in fact the number on the withdrawal forms was for a different state than the one in which the owner resided). SBL's investigation later discovered the form indicated to send the funds by EFT to a bank also in a different state than the one in which the owner resided.

Less than a week prior to the first SSW, an Electronic Authorization had been submitted that included the same differing signature and telephone number for the owner.

Another Scheduled Systematic Withdrawal request for the same contract was received several months later that also included the same differing signature and telephone number for the owner. The form was accompanied by a voided check that was a previously used check (it is rare for someone to use a used check as a voided check). Also notable is the signature on the voided check was whited out.

SBL reimbursed the customer, and so SBL lost a substantial amount of money as a result of these fraudulent withdrawals.

The signature discrepancies on the SSW forms were clear red flags that the transactions requested were suspicious. The different telephone number for the owner indicated on the SSW forms was also a red flag, as was the voided check sent with the subsequent SSW request.

While not as apparent as the signature discrepancies, the different telephone number for the owner, or the voided check, the multiple SSW requests received for the contract is also suspicious. Receiving multiple SSW requests, especially within a relatively narrow timeframe, is very unusual and suggests that the actual person submitting the requests was not familiar with what an SSW is as opposed to a one-time withdrawal request (something the owner of the contract can reasonably be expected to know).

3. SBL received a withdrawal request by fax, the cover page for which showed two different fax numbers in different area codes (neither of which corresponded to the area code for the customer's telephone number we had on file). The daytime telephone number for the customer given on the withdrawal form also did not match the customer's telephone number on file (including having a different area code).

On the withdrawal form, the customer's purported signature included her middle name which was not included in the signature we had on file for her. The purported signature for her husband in the Community Property section of the form also included his middle name (people typically do not include their middle names in their signatures). Additionally, the same signature written on the line for the Financial Advisor was written in the TPA signature block with "Mr" written on the title line (a legitimate financial advisor/registered representative would know not to sign in this section and that the title referred to the signer's position, not the title Mr., Mrs., etc.).

4. A loan application was submitted for a 403(b) variable annuity requesting a very large loan. The loan request form included a telephone number that did not match the telephone number for the customer we had on file. A call to that number was made to advise that the requested loan amount exceeded the maximum permissible loan amount: the imposter on the call told us to proceed with the loan. The funds were wired to a bank in a different state than the state in which the contractowner resides.

Account Takeover & Identity Theft

Identity theft occurs when a thief uses another person's personal identification—name, address, Social Security number, date of birth, mother's maiden name, or other identifying information—to open new credit card accounts, obtain loans in the victim's name, open new checking, savings, or investment accounts using the victim's name, or lease cars and apartments. To illustrate how significant a problem Identity Theft has become, by one estimate there are now more than 14 billion stolen identity records on the "dark web" (which can be bought and used for the malicious purposes described here).

Identity theft ruins reputations, destroys credit ratings, and empties bank accounts. Fraud artists sweep up personal information, take on the personas of victims and steal money from their accounts, or rack up bills in their names. It's one of the fastest growing white-collar crimes, fueled by the exponential growth of the Internet and instant credit as well as widespread use of Social Security numbers. Security Breaches at Equifax and the IRS, among others, made available to criminals the personal information of tens of millions of consumers and thus made all of those consumers vulnerable to identity theft.

Account Takeover is the use of an individual's stolen identity information by a criminal to steal money, e.g., fraudulently withdrawing funds from an annuity owner's contract. Account Takeover is one type of consequence of Identity Theft: while Identity Theft is the act of stealing a person's personally identifying information and, in most instances, using that stolen personal information to open new accounts, contracts, etc. in the victim's name, Account Takeover is the use of stolen personal information to steal money from an account or contract that the victim had already opened.

Types of Fraud Perpetrated by Identity Thieves

- Credit/debit card fraud
- Check fraud
- Bank fraud
- Computer & telecommunications fraud
- Social program fraud
- Mail fraud
- Government documents or benefit fraud
- Insurance and mortgage fraud
- False identification fraud
- Wire transfer fraud

Account Takeover & Identity Theft

Examples of Red Flags

- The application appears to have been altered or forged
- The "owner" has trouble answering the security questions on the telephone
- A customer says he/she has not received confirmations/statements (could have been intercepted in the mail, etc.)
- A withdrawal request form that includes a telephone number for the owner that does not match the telephone number we have on file for the owner
- A void check accompanying a withdrawal request is missing standard features such as the padlock or camera symbol that indicates security features are present, MP notation on the signature line, etc.
- Customer claims to be unaware of withdrawal activity that has occurred on his/her account or contract
- Unauthorized address changes, or an address or telephone number change request within a short time before a withdrawal is requested
- The owner signature on a withdrawal request form is significantly different than the owner's signature we have on file

An example of account takeover at Security Benefit:

An agent copied a client's signature to partial withdrawal requests and had the money deposited into his personal bank accounts. However, the agent said the bank account was the client's on the withdrawal form in order to avoid suspicion. (*forgery was used to carry out this fraud.) In addition, the claims fraud example associated with Scheduled Systematic Withdrawals on a previous slide also involved account takeover.

Internal Fraud

Internal fraud is considered to be any misappropriation of funds, securities, supplies or other assets, the disappearance of furniture, fixtures, and equipment, or knowingly making false entries in company books, records and statements with the intent to deceive.

Red Flags

- Significant, observed changes in behavior patterns
- Inadequate income for lifestyle
- Excessive gambling or other speculative behavior
- Undue desire for self-enrichment and personal gain
- Emotional trauma in home life or work life
- Noncompcompliance with corporate directives and procedures

Am I really in the position to detect fraud?

Cynthia Cooper, the famous whistleblower at WorldCom, gives the following advice for fraud detection, "When someone is hostile or acting in a manner that is out of character, you should ask yourself why. Listen to your instinct. If something doesn't feel or seem quite right, it might not be. If people are acting out of character or appear to be working to head you in another direction, step back and ask yourself why.

Healthy skepticism, good judgment and intuition are the keys to fraud detection. You can only spot an irregularity if you already know the norms.

Don't always take things at face value. If something seems suspicious, ask yourself why. As a career criminal once said, "I am always thinking, 'what kind of answer can I give you, to satisfy you so that I can go on and you'll go on?

Most fraud is detected through tips from employees, suppliers, customers, or anonymous sources.

It is vital to identify small issues before they become larger.

When transaction volume rises and processes become more complex, fertile ground can be laid for a fraudster. With new technology, system conversions, or a large amount of work, the priority becomes simply ensuring the transactions are processed, with little time left for verifying their accuracy. ***It is important to pay attention to detail while processing transactions; otherwise, red flags could pass by undetected.***

According to the former national Anti-Fraud Director for Blue Cross and Blue Shield, "Three things are important [in fraud detection]: pay attention to detail, every piece of evidence is important, and good luck is not random—it is a byproduct of preparation and perseverance."

Security Benefit Special Investigative Unit (SIU)

Security Benefit has established a committee designed to accomplish the goals of the Anti-Fraud Plan.

The SIU's goals include:

- Ongoing employee training
- The establishment of specific procedures to prevent fraud
- To provide a means to investigate suspected fraud
- The reporting of fraud to appropriate law enforcement authorities
- Ensuring cooperation in the prosecution of fraud cases
- The reporting of fraud-related data to state insurance regulators as appropriate

The SIU consists of the following members:

- Chief Compliance Officer (Carmen Hill – Ext. 3341)
- Internal Auditor (Jeanne Slusher – Ext. 3620)
- SB Operations (Rich Wells – Ext. 3408)
- SE2 Operations (Kevin Paulson; Scott Geraghty, designee – Ext. 3586)
- Human Resources consultant (Jennifer Purvis – Ext. 3538)
- Internal attorney (Chris Swickard – Ext. 3321)
- Other members (Greg Garhart – Ext. 3203)

These extensions can be reached from outside the Company by calling 800-888-2461 + Ext. or 785-438-3000, option 1 + Ext.

How to report known or suspected fraud?

If you suspect fraud:

- **Do not alert the suspect you are suspicious**
- Take notes regarding your suspicions
- Do not investigate on your own—associates should not attempt to conduct individual investigations, interviews, or interrogations in order to determine whether or not a suspected activity is, in fact, improper
- Contact your manager to escalate the issue to the Compliance Department (*if you are an SE2 employee working for a non-Security Benefit client, contact your block's client relationship manager)
- Directly contact the Compliance Department by contacting the Chief Compliance Officer (Carmen Hill)

What will happen after you report a suspected fraud?

1. The Chief Compliance Officer will review all available information regarding the suspicious activity. Depending on the magnitude and seriousness of the potential fraud, the Chief Compliance Officer may notify the members of the SIU.
2. Temporary instruction may be given regarding how to handle the account/contract (i.e. block transactions, apply a password, etc.).
3. A complete investigation will be conducted by the SIU, if appropriate. Employees and other individuals may be interviewed regarding the account/contract to determine more detailed information.
4. The fraud may be reported to applicable law enforcement or regulatory agencies, if appropriate or required. For example, the California Insurance Department requires reporting to its Fraud Division within 60 days of reasonable belief that fraud was committed.

What if someone contacts me regarding a fraud case?

All requests for information and/or assistance from governmental agencies, regulators, or law enforcement regarding fraud should be immediately forwarded to the Chief Compliance Officer (or your block's client relationship manager) as indicated in the steps listed above. It is the company's policy to comply with applicable laws and regulations and to respond properly to all contacts, inquiries, or requests made by the authorities; therefore, it is important to forward these requests immediately.

Anti-Money Laundering Training

Background of AML Requirements

- Federal and state laws and regulations require financial institutions to respond to the growing threat of money laundering by establishing anti-money laundering programs.
- The ***Bank Secrecy Act*** of 1970 (BSA) was the first major piece of legislation aimed at preventing and detecting money laundering. The BSA sets forth many recordkeeping and reporting requirements designed to help track large or unusual financial transactions. The **Financial Crimes Enforcement Network** (FinCEN), a division of the U.S. Department of Treasury, is responsible for monitoring compliance with the Bank Secrecy Act.
- The ***USA PATRIOT Act*** (**U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act) of 2001 created new requirements for financial institutions to combat money laundering activity by requiring the establishment of AML Programs, Customer Identification Programs, and other information sharing regulations.

USA PATRIOT Act

The most recent attempt to curb money laundering came in October 2001 with the passage of the USA PATRIOT Act. This law was passed as a result of the September 11, 2001, terrorist attacks and greatly strengthens anti-money laundering laws, enhances civil and criminal penalties for violations, and grants new law enforcement powers and surveillance capabilities. It also significantly strengthens earlier anti-money laundering laws by imposing new obligations on financial institutions, including insurance companies. The Act also amends the original Bank Secrecy Act and existing criminal statutes covering money laundering.

The *USA PATRIOT Act* requires financial institutions, including insurance companies, to:

- Establish and implement policies, procedures, and controls that can reasonably detect suspicious activities (procedures should include a reporting mechanism for reporting suspicious transactions);
- Designate an AML Compliance Officer (Greg Garhart), either an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program;
- Conduct ongoing employee training; and
- Have an independent audit function test the program periodically.

The following Security Benefit companies have AML Programs:

- **S**ecurity **D**istributors, LLC,
- **S**ecurity **B**enefit **L**ife Insurance Company, and
- **F**irst **S**ecurity **B**enefit **L**ife Insurance and Annuity Company of New York.

The Programs are updated and amended periodically as necessary.

Money Laundering Basics

Money laundering is the process of making cash from illegal activities appear as if it has come from legitimate sources. The purpose is to conceal the true source of the funds so the laundered funds can be used freely.

The two major reasons for laundering money are to:

1. Conceal money generated from illegal activity (drugs, gambling, etc.)
2. Hide money from the IRS in order to evade taxes

The three phases of money laundering are:

1. ***Placement*** of funds into financial institutions. Large amounts of cash are placed in domestic or offshore banks (insurance companies generally don't accept cash). In order to avoid currency reporting requirements, the money launderer can "*smurf*" the funds. "*Smurfing*" is the process of breaking transactions up into smaller amounts to evade reporting requirements. Sophisticated smurfing operations may involve hundreds of bank accounts in dozens of cities.
2. If the placement of the initial funds is undetected, funds are ***layered*** in various financial transactions to confuse and complicate the audit trail.
3. The final phase is the ***integration*** of assets back into the economy as an apparently legitimate business transaction.

Effective money laundering schemes rely on creating complex paper trails. More steps may make the tracing of funds more difficult, but it also increases the chance that a transaction will be reported somewhere.

Sources of Illicit Funds

- Corruption
- Drug trafficking
- Tax evasion
- Bankruptcy fraud
- Attempts to avoid collection of judgments
- Concealment of assets from creditors or spouses
- Avoidance of duties and tariffs
- Terrorist financing

Once deposited in the financial institution, the illicit funds can be wired or otherwise sent to other accounts and through various front companies, nominees, or trusts until they arrive at their ultimate destination.

Money Laundering Example

We no longer accept *cash*, *money orders*, *third party checks*, *credit card checks*, *money market checks*, *starter checks*, or *traveler's checks* without a valid reason. *Supervisor approval must be obtained prior to acceptance and processing. Supervisor approval must also be obtained for cashier's checks over $150,000 under Mail Operations Cashiering Guidelines.*

Because insurance companies do not usually receive from contract owners significant amounts of currency (if any), insurance companies are not as likely as banks to be used in the initial stage of the money laundering process. However, money launderers may use insurance products in the "*Layering*" and "*Integration*" phases.

Money launderers go through all the trouble of layering funds so that they can get a check from a reputable institution and complicate the trail of illicit funds.

Money Laundering Red Flags

Operations personnel are in a unique position to spot many kinds of unusual account activity. The following red flags should be considered when processing transactions.

Customers Who Provide Insufficient or Suspicious Information

- A customer who uses unusual or suspicious identification documents that cannot be readily verified
- A customer who exhibits unusual concern for secrecy as to his or her identification or business or who delays providing identifying documents and information
- A business that is reluctant, when establishing a new account, to provide requested information about the business, such as corporate resolutions, the names of its officers and directors, or information on its location
- A customer's home or business telephone is disconnected (especially soon after opening an account)

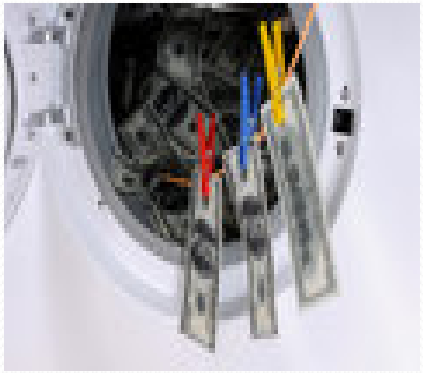
- A customer who is a trust or shell company that is reluctant to provide information on controlling parties and underlying beneficiaries (Beneficial owners hire nominee incorporation services to establish shell companies and open financial accounts for those shell companies while shielding the owner's identity)
- A customer who refuses to identify or fails to indicate any legitimate source for his/her funds and other assets
- Customer(s) who open multiple accounts in the same or different names and then conduct numerous transfers among the accounts
- No apparent relationship between the owner and the insured/annuitant and/or between the owner and the beneficiary
- Customer is hard to reach; he/she always calls you
- Unusually high number of contracts for a particular customer
- Change of address, beneficiary or ownership, followed by a large payment

Efforts to Avoid Reporting or Recordkeeping Requirements

- A customer asks about reporting requirements (such as *Currency Transaction Reports ("CTRs"), Form 8300s, SARs*, etc.)
- A customer asks to be exempted from reporting recordkeeping requirements (we are not able to exempt anyone from the reporting requirements)

Funds Transfers

- Many fund transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts
- Fund transfer activity occurs to or from a financial secrecy haven, or to or from a high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history
- Wire transfers to or from a geographic location that doesn't make sense for that customer
- Fund transfer activity is unexplained, repetitive, or shows unusual patterns
- Multiple withdrawals in a short period of time and/or withdrawals being wired
- Customer using same withdrawal form more than once and apparently only changing the date
- Fund transfers are sent or received from the same person to or from different accounts
- Change of bank account followed by a large withdrawal request



Other Possibly Suspicious Activity

- Structured transactions (i.e. a series of transactions in amounts less than $10,000, especially amounts just under $10,000, e.g., $9,500)
- A customer who makes a funds deposit followed by an immediate request that the money be withdrawn — a pattern of premium/withdrawal/premium/withdrawal
- A customer's account shows an unexplained high level of account activity
- Early termination of a product, especially at a cost to the customer
- A customer who shows little concern for the investment performance of a product but much concern about early termination features
- A customer who exhibits a lack of normal concern for investment risks, surrender charges, commissions, or other costs
- Numerous transactions involving cashier's checks, currency, or similar monetary instruments aggregating to significant amounts (remember, we do not typically accept these forms of payment)
- Wire transfers coming from the current (or new) broker/dealer or representative. Could the representative have received cash from the customer, deposited it into his/her account, and forwarded the money to SB?
- The transfer of the benefit of a product to an apparently unrelated third party
- A customer who borrows the maximum amount available soon after purchasing the product
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them

Spotting a red flag does not mean there is a problem with a customer or contract, but it does mean that you should follow up. Follow the procedures discussed later in the training for bringing the red flag to attention through the proper channels.

What to Do When You Suspect a Suspicious Transaction?

- If discovered during a phone call, take detailed notes about the conversation and identifying information in order to find the recorded call later on (number from which the call was made, time of call, date, name of person you are speaking to)
  - Stay calm—do not alert or tip off the customer that you think they are acting in a suspicious manner
  - Do not try to conduct an investigation yourself or answer questions you do not know the answers to
  - If you suspect suspicious activity, provide timely notification to your manager, or the AML Compliance Officer (**Greg Garhart**), or another member of the Compliance Department (*if you are an ***SE2 employee*** working for a non-Security Benefit client, you should refer suspicious activity to your block's client relationship manager)

Money Laundering and the Insurance Industry

The expansion from insurance policies to investment products has substantially increased the money laundering threat posed to the insurance industry. The introduction of investment products to the insurance portfolio has broadened the potential customer base for insurers and agents and has created new transaction patterns.

Money launderers exploit the fact that insurance products are often sold by independent brokers and agents who do not work directly for the insurance companies. These intermediaries may have little know-how or incentive to screen clients or question payment methods. In some cases, agents take advantage of their intermediary status to collude with criminals against insurers to perpetrate fraud or facilitate money laundering.

Annuity contracts contain the risk a money launderer will exchange illicit funds for an immediate or deferred "clean" income stream. Further complicating AML practices, the policyholder, or purchaser of an insurance contract, may not be the beneficiary or even the subject of the insurance coverage. The potential for multiple parties to be involved in a single contract often makes it difficult to perform customer due diligence.

The cash surrender value of a life insurance policy or annuity contract is often much less than the amount paid in because of liquidation penalties, particularly if the policy has only been in existence a few years. But from the money launderer's perspective, the liquidation penalty (surrender charge) is, in effect, a cost of doing business.

Trusts

Trusts separate legal ownership from beneficial ownership and are useful when assets are given to minors or individuals who are incapacitated. The trust creator transfers legal ownership of the assets to a trustee, which can be an individual or a corporation. The trustee manages the assets on behalf of the trust beneficiary(ies) based on the terms of the trust documents.

Although trusts have many legitimate applications, they can also be misused for illicit purposes. Trusts enjoy a greater degree of privacy and autonomy than corporate vehicles. Trusts can conceal the identity of the beneficial owner of the assets and often constitute the final layer of anonymity for those seeking to conceal their identity.

It is important to receive the required documentation for the trust when setting up a new contract. Delay or failure to provide trust documents may need to be questioned.

Exception Reports

Designated personnel in the Operations area receive month-end reports that highlight account activity exceeding certain thresholds established during the development of the AML Program. There are several reports that are currently reviewed:

A. Excessive transaction activity/significant dollar amounts
B. Unusual wire activity
C. Accounts opened with addresses outside the United States
D. Annuity contracts exercising the free look right

CIP ("Know Your Customer")

Section 326 of the PATRIOT Act expands the Bank Secrecy Act by requiring Financial Institutions to implement Customer Identification Programs (CIPs).

CIPs must include procedures for:

- Verifying the identity of any person seeking to open an account to a reasonable and practicable extent.
- Maintaining records of the information used to verify a person's identity, including name, address, and other identifying information.
- Consulting lists of known or suspected terrorists or terrorist organizations to determine if the person seeking to open the account appears on any such list.

The move away from face-to-face account opening and account access creates more opportunity for fraud, identity theft, and money laundering. The world is shifting to processing business electronically rather than in person and on paper. Such conditions make CIPs even more important. The ultimate goal of a CIP is for the organization to feel comfortable knowing that the persons opening accounts are really who they say they are.

CIP – Information to Collect

- Name
- Date of birth
- Address (if PO Box is given, a residential address is also required)
- Identification number (ex: Social Security Number, tax ID, or passport number)
- Other identifying documentation for non-natural owners (trusts, corporations, etc.)

If customers refuse to provide the required information or appear to provide misleading information, an account or contract should not be opened. You should notify the AML Compliance Officer (**Greg Garhart**) (*If you are a SE2 employee working for a non-Security Benefit client, you should refer suspicious activity to your block's client relationship manager.) so that the situation can be evaluated in regard to suspicious activity reporting.

Reliance on Third Parties

Selling agreements with independent broker/dealers, general agents, and other third parties have been negotiated to include the requirement that the independent party will conduct the CIP when selling Security Benefit business. These independent parties are required to annually certify that they are following the AML Program requirements of the *USA PATRIOT Act* and are executing such procedures when selling Security Benefit products.

CIP Conducted by Security Benefit

Security Benefit must conduct CIP on the NEA Direct Invest product, the direct sold EliteDesigns product, and other instances as outlined in the operating guidelines. Information can be analyzed through documentary evidence, non-documentary evidence, or both.

Documentary evidence – physical verification of customer identification documents (usually performed by the retail broker/dealer or independent agent):

- **Individuals**
  - A current driver's license
  - Passport or other government-issued identification
- **Non-Individuals**
  - Certified copies of Articles of Incorporation
  - Government-issued business license
  - Partnership Agreement
  - Trust Instrument

Non-documentary evidence –

- Identity verification software
  - Reports generated that highlight inconsistencies in the identifying information (Address Screener, TransUnion)
- Contacting a customer
- Other sources

The majority of Security Benefit customers' identities are verified using identity verification software (when not relying on a third party to conduct the CIP).

OFAC

The ***Office of Foreign Assets Control*** (OFAC) is not a post-9/11 agency; in fact, it has been around for over 30 years. It is an agency within the U.S. Department of Treasury and is charged with administering and enforcing U.S. sanction policies against targeted non-U.S. organizations and individuals who sponsor terrorism and international narcotics traffickers. OFAC maintains a list of individuals, governmental entities, companies, merchant vessels, and countries around the world that are known or suspected to engage in illegal activities. These persons or entities on the OFAC list are known as *Specially Designated Nationals and Blocked Persons* (SDNs).

Companies have the obligation to run their database lists against the OFAC list on an ongoing basis, because customer lists and policyholder lists won't remain stagnant, and more importantly, the OFAC list does not remain stagnant.

Security Benefit routinely compares its customer base to the OFAC list to ensure there are no positive matches or regulatory reporting requirements. If a positive match is found, the AML Compliance Officer (Greg Garhart) will determine whether the account/contract needs to be blocked or closed. The AML Compliance Officer will notify OFAC of a positive match within 10 days of discovery.

***We cannot notify the customer that his/her account/contract has been blocked.*

CTRs and Form 8300

IRS Form 8300 must be filed when the company receives more than $10,000 in cash in one transaction or in two or more related transactions. If more than one cash payment for a single transaction or for related transactions is received, the company must report the multiple payments any time the total amount received exceeds $10,000 cash within any 12-month period. The company must keep records on wire transfers of $3,000 or more, including the names of the transmitter and the recipient. The company must also verify the identity of transmitters and recipients who are not established customers.

FinCEN's Currency Transaction Report (CTR) is very similar to the IRS Form 8300. The type of organization filing the report determines which form must be filed. There is a move in the insurance industry to make amendments to the currency transaction forms.

Since Security Benefit does not generally accept cash or cash equivalents, Form 8300s and/or CTRs are rarely filed.

The Compliance Department will determine which form is appropriate if such a filing needs to be made.

Suspicious Activity Reports (SARs)

Since 1996, various financial institutions have been required to file Suspicious Activity Reports, which are used to alert law enforcement and other regulatory organizations about suspicious transactions relevant to possible money laundering or other violations of law.

The following types of activity may trigger a SAR filing (the transaction must involve at least $5,000 to be filed as a SAR):

- A transaction that involves funds derived from illegal activities or is intended to hide or disguise funds or assets derived from illegal activities
- The transaction has no business or apparent lawful purpose
- The transaction is not the sort in which the particular customer would normally be expected to engage
- The transaction appears to have been designed to evade the Bank Secrecy Act reporting regulations
- A review of the back-end exception reports uncovers unusual account activity that, upon further examination, warrants a SAR filing

Notify the AML Compliance Officer (Greg Garhart) immediately if you have identified a situation in which a SAR may need to be filed (*if you are a SE2 employee working for a non-Security Benefit client, you should refer suspicious activity to your block's client relationship manager). The Compliance Department will review any activity that may trigger a SAR filing, make the determination whether a SAR should be filed, and if so, will file such SAR. A SAR must be filed within 30 days of detection. The Compliance Department will also keep documentation as to why a SAR was not filed (if decided) in regard to a reported suspicious transaction.

***It is against the law (a felony) to inform the suspected person(s) involved in the transaction that a SAR has been or will be filed.*

Case Studies

Case Study One – The Broker/Dealer

Beth worked at a large broker/dealer and had gotten several new customers within several weeks. However, she did not immediately verify the information required under her firm's customer identification policies, even though the customers all gave her the same business addresses for different occupations. The customers also opened their accounts with deposits from the same third party source. Eventually, when Beth verified the information she found that all the business addresses were the same, which were actually a post office box. Because she didn't want to lose the accounts, she waited several more weeks before telling her supervisor.

When her supervisor investigated the accounts, she found that the corporate names given to Beth were not legitimate business names. As a result, the firm closed the accounts and filed a Suspicious Activity Report (SAR). Before the accounts were closed, however, two customers had executed several structured transactions by depositing cash, cashier's checks, and money orders in amounts under $10,000. When considered alone, the transactions didn't seem out of the ordinary.

Later, Beth and the firm learned that these customers were using the firm as part of a much larger money laundering scheme. Federal authorities investigating the transactions repeatedly questioned Beth and her firm about the transactions. Because Beth waited several weeks to report the suspicious activities, she and her firm are now facing serious penalties. The firm, for example, may be liable for the amount of funds laundered, plus penalties, while Beth may face criminal charges for "*willful blindness*".

What exactly is ***willful blindness***?

Why might Beth also face criminal charges for "willful blindness"? What exactly does this mean? Today, the vast majority of courts adhere to a "willful blindness" standard to determine whether a person should have known that funds are criminally derived. What this means is that if a broker wasn't aware of the criminal source of a client's funds because he or she intentionally turned a blind eye to the facts and circumstances surrounding the transaction, a court may nonetheless find that the broker "knew" of the funds' criminal origin. Note that if a person is merely negligent or makes a mistake, such behavior won't rise to the level of "*willful blindness*."

In Beth's case, a good argument could be made that she was in fact "willfully blind" to the suspicious facts surrounding her new customers' accounts. For example, she failed to verify the customers' identities. When she did follow up several weeks later she discovered that they all gave her the same business address, even though they were supposedly engaged in different occupations. Another red flag that she initially ignored was that the customers all opened the accounts with deposits from the same sources, and that their supposed business addresses were actually post office boxes.

Case Studies

Case Study Two – The Insurance Company

Mark is a new representative of ABC Insurance Company, one of the oldest financial institutions in the U.S. One day, Tom walks into Mark's office and explains that he is a businessman and has made his money from investing in several restaurant franchises. He recently inherited some money from his parents' estate and wants to invest it in a variable annuity to shelter it from taxes.

When it comes time to fund the annuities, Tom wants to wire in $2 million to open the account. He promises to give Mark substantial business in the future. Mark then completes the sale and forwards the paperwork to the home office. Several weeks later, Mark discovers that Tom canceled the policy during the 10-day free look period. The insurance company refunded the $2 million via wire transfer to another bank. The result is? Tom now has $2 million of "legitimate" money, transferred from one of the country's leading insurance companies to another of his accounts. And, ABC Company and Mark now face potential liability for facilitating money laundering.

What were some of the red flags that Mark should have been aware of? First, the application simply looked too good. A common money laundering scheme used in the variable products industry is to purchase annuities with lump-sum cash payments and then cancel the policy during the free-look period. Although administrative expenses may be imposed, the money launderer now has an apparently legitimate source for his/her funds.

Mark also should have been suspicious of the fact that Tom never gave him personal information, was always in a big rush, and wasn't really concerned about other investment products. In addition, Tom didn't even want to know about the annuities' features other than the free-look period.

Criminal & Civil Sanctions

As seen in the two case studies, severe penalties can be imposed on both individuals and firms that violate the anti-money laundering laws. For example, criminal penalties include fines of up to $500,000 or twice the value of the property involved, whichever is greater. Prison sentences of up to 20 years can also be imposed. Civil penalties include fines of up to $10,000 or the value of the funds involved in the transaction, whichever is greater.

Additional criminal and civil penalties can be imposed under the Bank Secrecy Act, including up to 5 years imprisonment, a criminal fine of up to $250,000, or both. If the individual is violating the BSA as well as another law, or engaging in a pattern of illegal activity, a criminal fine of up to $500,000 can be imposed along with up to 10 years imprisonment, or both.

The USA PATRIOT Act adds additional criminal and civil penalties for violations of certain BSA provisions, including up to two times the amount of the transaction, or $1,000,000.

The Need to Understand Anti-Money Laundering Laws

Although most people in the financial services industry may be aware of anti-money laundering laws, many do not fully comprehend all of the implications involved in participating in transactions involving criminally derived proceeds.

For example, as shown in the first case study, failing to ask a client certain questions or ignoring some “red flags” may be considered to be “willful blindness” in a money-laundering prosecution.

Conclusion

Given the world we live in today, questions that might once have been considered inappropriate are now considered absolutely necessary. Employees who choose to ignore red flags do so at their own peril, possibly subjecting themselves and their firms to criminal and civil prosecution.

Additionally, the USA PATRIOT Act increased both the civil and criminal penalties that can be imposed for violating anti-money laundering laws. Given the increased terrorist attacks worldwide, the U.S. government and its agencies have made money laundering a higher priority, hoping to find and root out money launderers.

Even if a person unwittingly participates in a money laundering scheme, the resulting negative publicity can be devastating for both the individual and firm. Attempting to salvage one’s reputation after it is discovered that a broker or firm has knowingly or unknowingly facilitated a money-laundering scheme can be difficult, if not impossible, to do.

In order to protect both oneself and the company he or she represents, it is imperative to understand customer identification requirements, suspicious activity reporting requirements, as well as the other existing anti-money laundering regulations.

THE END