

INVESTIGATING AND ADJUSTING EMPLOYEE DISHONESTY CLAIMS

Presented by Charles R. Franklin¹

1. EMPLOYEE DISHONESTY CLAIMS

- a. What Comprises Employee Dishonesty: dishonest acts, embezzlement, forgery, robbery, burglary, computer fraud, wire transfer fraud, counterfeiting, and other criminal acts.
- b. Concerns when Investigating a Claim:
 - i. whether an employer has applicable insurance coverage;
 - ii. whether evidence exists to sufficiently prove the dishonest act;
 - iii. whether the dishonest act is covered by the insurance policy; and
 - iv. negotiating and settling any payment made under the policy.

2. TYPES OF COVERAGES

- a. Employee Dishonesty Policy → generally covers only thefts by employees (separate insurance is often needed for independent contractors)
 - i. Investigation
 1. Verification that the Suspected Individual is an Employee of the Insured:
 - a. Federal Tax Form W-2: Wage and Tax Statement
 - b. Employee's Employment File.
 2. Isolate the Loss to the Suspected Employee:
 - a. Once the insured provides financial documents evidencing lost assets, those lost assets may be covered under an employee dishonesty policy only if they are traced to a specific individual.

¹ Charles R. Franklin is a partner at Belongia, Shapiro & Franklin, LLP. Since 1980, Charlie has concentrated in general civil litigation, fraud, and first and third-party defense, recovery and other insurance-related work. He is experienced in representing professional real estate appraisers and property inspectors in malpractice claims, lawsuits and disciplinary hearings. Charlie counsels clients (both companies and policyholders) on insurance coverage and presentation of claims. He has successfully argued before the Illinois Supreme Court on a case involving exculpatory provisions in a contract. Charlie also often serves as a "neutral" or independent arbitrator in various matters.

Charlie earned his Bachelor of Arts in Asian Studies from the University of Michigan, and his Juris Doctor from the University of Miami (Florida) School of Law. He is "AV Preeminent" rated with Martindale-Hubbell. Charlie is a past president of the Casualty Adjusters Association of Chicago, and was a founder and former board member of the Claims Association of Greater Chicago.

- i. Examine the suspected employee's job duties/responsibilities, including which records the employee could access.
 - ii. Ensure the thefts only occurred on the days that the employee worked or had remote access and that the employee's job duties provided an opportunity to commit theft and/or manipulate financial records.
 - iii. Confirm that the loss was not a "mysterious disappearance" or a general / unknown inventory shortage.
 3. Obtain Information from the Suspected Employee:
 - a. Before concluding an investigation, when possible, obtain police reports, interview those involved, or obtain copies of signed statements or confessions. These documents may help fill in gaps from the investigation and can support investigation conclusions if litigation ensues.
- b. Employee Dishonesty Bond → guarantees that the bonded employee will handle his/her employer's money and property with fidelity, and reimburses employers for losses from employee fraud or theft of an employer's cash and other property.
- c. Fidelity Bond → protects employers from any loss of money or property incurred as a result of an employee's dishonesty or fraudulent acts and indemnifies the principal for losses caused by the dishonest actions of its employees.
 - i. Individual Bond or Scheduled Bond
 1. Individual Bond covers specific employees.
 2. Scheduled Bond covers specific positions or name employees, such as all employees of a retail store, or all cashiers.
 - ii. 3 Parties Typically Involved in a Claim under a Fidelity Bond:
 1. Principal might cause the loss; Employer/Policy Holder would collect if the Principal causes the loss; and a Surety is the entity that pays the value of the loss to the Employer.
 - iii. Investigation
 1. Establish the Facts
 - a. Identify and obtain supporting documents; prepare an analytical timeline and flow chart; obtain statements from those involved or with knowledge; and prepare a written documentation of how the employee theft was conducted and discovered.

1. When is it filed? → there are two different dollar thresholds that require a SAR, depending on the stage of discovery and the type of transaction involved.
 - a. \$2,000 back-door threshold applies if a customer is conducting or attempting to conduct a transaction aggregating to \$2,000 or more (front-door is face to face with the customer).
 - b. \$5,000 threshold applies for transactions identified by issuer of money order or traveler's checks from a review of clearance records.
2. What is included in the Narrative Section of the Report?
 - a. Description of what is unusual, irregular, or suspicious about the alleged fraud;
 - b. Description of the conduct that raises the suspicion;
 - c. Explanation of whether a transaction was attempted or completed;
 - d. Explanation of who benefits from the transaction;
 - e. Description of the alleged subject and any information gathered from that person;
 - f. Including of any correspondent bank name and account information; locations of business entities; names of cities, countries and foreign financial institution linked to the transaction, especially if funds transfer activity is involved; and account numbers and beneficiary names.
- ii. Currency Transaction Reports (CTRs)³ → must be filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to a financial institution, which involves a transaction in currency of more than \$10,000.
 1. Multiple currency transactions are treated as a single transaction if the financial institution has knowledge that: (a) they are conducted by or on behalf of the same person; and, (b) they result in cash received or disbursed by the financial institution of more than \$10,000. (31 CFR 103.22).
- iii. International Transportation of Currency or Monetary Instruments Reports (CMIRs)⁴ → any person (including a bank) who physically transports, mails or ships, or causes to be physically transported, mailed, shipped or received, currency, traveler's checks, and certain other monetary

³ http://www.fincen.gov/forms/bsa_forms/#CTR (accessed October 20, 2010).

⁴ http://www.fincen.gov/forms/bsa_forms/#CTR (accessed October 20, 2010).

instruments in an aggregate amount exceeding \$10,000 into or out of the United States must file a CMIR.

- iv. GAAP – Generally Accepted Accounting Principles:
 - 1. Aggregate set of standards on how to account for various transactions.
 - 2. Financial reporting should provide information potentially used to analyze an employer’s balance sheets or an employee’s alleged dishonest acts.
 - 3. GAAP generally precludes a financial institution from recording a receivable for a claim filed under a fidelity bond until it has determined that collection is highly probable, and it can estimate the recoverable amount with considerable accuracy.
- v. KYC – Know Your Customer:
 - 1. Financial institutions must (i) verify the identity of new account-holders, (ii) ensure that the institution has a reasonable belief that it knows each customer’s identity, and (iii) compare the names of new customers against governmental lists of known or suspected terrorists or terrorist organizations.
 - a. These procedures create a record of the life of the financial institution’s relationship with a customer and may be referenced when investigating allegedly dishonest or fraudulent acts.

3. ADJUSTING CLAIMS IN LIGHT OF THE SUBPRIME CREDIT CRISIS

- a. Lending practices that contributed to the subprime credit crisis are resulting in complex employee dishonesty claims.
 - i. These claims require a thorough understanding of internal controls, redundancies and underlying financial documents.
 - ii. Investigation:
 - 1. Identify the amount stolen and the applicable policy period;
 - 2. Confirm whether the employee acted alone or colluded with others; and
 - 3. Isolate the amount of property actually stolen from the amounts stemming from accounting irregularities.
 - 1. *Since claims stemming from subprime lending are often flooded with complex financial documents, an adjuster may consider consulting a forensic accountant to ‘follow the funds’ to identify the precise cause of the loss.

4. GENERAL BEST PRACTICES FOR CONDUCTING A DILIGENT CLAIM INVESTIGATION

- a. Two Basic Purposes: Investigate and Verify
 - i. Investigate – gather all relevant information to determine exactly what happened during the alleged fraud.
 - ii. Verify - confirm allegations, events, damages, and property losses with as many sources as needed.

- b. Road Map → Timely Notification of Loss; Verification of Coverage; Thoroughly Investigate; Contact and Interview any Claimants and Witnesses; Diligently Follow-up; Loss Assessment; Timely Negotiation, Settlement and Payment.

- c. Other Considerations
 - i. Focus areas when balancing an insured’s concerns about controlling the cost of an investigation with an adjuster’s duty to investigate diligently:
 1. Document Analysis: Since there is usually a large volume of electronic and hard copy documents available, efficiently separating those with probative value from those that form the ‘haystack’ can significantly lower costs. Computer forensics can accelerate the investigation, for example by locating hidden or deleted files and “smoking gun” e-mails.
 2. Interviews: Identify individuals well-placed to provide as much information as possible. Who could be confiding in whom? Who is positioned to know the facts and where any potential evidence could reside? Will interviews be information-gathering or admission-seeking?
 - a. *After being informed of an alleged loss, too much time spent on preparation to investigate may look like delay, especially when scheduling interviews. Timely interviewing is crucial: memories fade, stories spread, and witnesses may end up being influenced by other parties involved.
 3. Asset-Tracing: Computer forensics and data analytics is highly valuable, because technology has revolutionized the ways in which to track related parties or those who spend well beyond their means.
 - ii. Red flags to consider when investigating
 1. Employer never calls in sick regardless of how physically ill he/she appears;
 2. Employee never takes vacation time;



3. Employee's lifestyle has improved greatly without explanation;
4. Certain employer records have become untraceable;
5. Employee engages in excessive cash transactions on employer's behalf;
6. There are inventory shortages;
7. Invoice totals are rounded to whole dollar amounts;
8. Invoices lack proper company letterhead;
9. "Originals" are never used or cannot be found, or only photocopies can be produced;
10. Beware of photo-shopping, plagiarized forms and signatures, and the many varieties of identity theft; and
11. Make sure everything can be documented – check sources.