



# PERSPECTIVES

---

## **Fidelity Investigations: A Comprehensive Guide to Successful Claims Outcomes**

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

## INTRODUCTION: UNDERSTANDING FIDELITY INVESTIGATIONS

Fidelity / Crime / Financial Institution Bonds, in a general sense, cover an insured from the willful theft of property, money, and securities by one of their employees or an outside third-party carried out through a variety of means. Such fraud can impact myriad industries. However, typical industries affected by employee fraud, along with examples, include but are not limited to:

- Retail – Overpriced store leases, stolen inventory, no-bid advertising contracts
- Healthcare – Procurement fraud of healthcare equipment
- Hospitality – Theft of inventory
- Finance – Custodial funds stolen by a broker
- Credit Union – Employee faithful performance failure or loan program losses
- Technology – Embezzlement of funds from a tech company
- Education – Theft of high-end copier equipment from a state university system
- Non-Profits – Stolen tuition, grants, and payment of personal bills
- Government – Insider dealing with large contracts, pay raises, and vendor payments
- Manufacturing – A theft ring stealing OEM parts and selling out the back door.

This article will provide fundamental aspects of a fidelity investigation, from inception to recovery of stolen funds. This information is primarily intended to assist:

- claims examiners,
- inside and outside counsel,
- risk managers,
- brokers,
- claim executives who oversee fidelity claims,
- corporate investigation groups faced with employee theft losses.

## PRELIMINARY STEPS IN A FIDELITY CLAIM INVESTIGATION

When a fidelity claim is being filed, there are several initial steps normally taken by counsel and / or the carrier. For each claim, it is necessary for counsel and / or carrier to first carefully review the terms and conditions of the fidelity policy to understand specific coverages, limits, exclusions, and general policy conditions. Policies vary across organizations, so it is important to understand each organization's needs and for brokers and risk managers to ensure that the appropriate coverage is in place before the need arises.

As the financial investigators assisting a party at interest to a fidelity claim matter, they defer all coverage interpretation and decisions to counsel and / or carrier. However, the investigators must be familiar with all aspects of the fidelity policy before commencing any probe.

Some other determinations counsel and carrier make include determining the date of discovery and any subsequent claimed losses, determining whether or not the loss agent has ownership interest in the insured entity. They also verify dates of employment of the loss agent and whether that individual had any prior theft issues known to the insured. They also determine whether the insured has had continual coverage and if so for how long and at what coverage limits per section. They also review for additional coverages like claim preparation expenses as well as responsibilities of insured and insurer. The counsel and / or carrier also must be cognizant of any potential subrogation recovery possibilities.

## TYPES OF FIDELITY INSURANCE CLAIMS OR LOSSES

Fidelity insurance protects organizations from financial losses resulting from acts of dishonesty or fraud committed by their employees or third parties. Most fidelity insurance policies provide coverage for the following types of claims:

- **Internal Fraud: Employee Dishonesty or Theft:** This is the most common type of fidelity claim as it covers losses resulting from internal fraud, such as theft, embezzlement, computer fraud, forgery, and funds transfer fraud schemes, committed internally by an organization's employee. Some of the fraud schemes often perpetrated include payroll, vendor or accounts payable procurement fraud, cash and sales / accounts receivable schemes, and theft of physical assets like inventory, equipment, and machine parts.
- **Forgery or Alteration:** These claims cover losses resulting from the forgery or alteration of financial documents, such as checks, promissory notes, purchase orders, and contracts such as signing the controller's name to falsely prepared accounts payable checks.
- **Computer Fraud:** This type of claim covers losses resulting from computer-related fraud, including social engineering (phishing attacks), hacking, or unauthorized access to the organization's computer systems. Computer fraud claims under fidelity insurance policies have grown over the years as more companies find themselves victims of cyber breaches.
- **Funds Transfer Fraud:** These claims cover losses resulting from fraudulent instructions to transfer funds. These may emanate from inside or outside of the company.
- **Money and Securities:** Fidelity insurance policies may provide coverage to the policyholder in the event of theft, disappearance, or destruction of money, securities, or other negotiable instruments. An example would be the theft of cash receipts.
- **Credit Card Fraud:** Some fidelity policies may include coverage for losses resulting from credit card fraud. Coverage may apply for fraudulent credit card transactions and be advantageous to organizations that process credit card payments. Using company credit cards for unauthorized personal purchases is a common scheme.
- **Third-Party Theft:** Fidelity insurance policies can also include coverage for losses resulting from theft or fraud committed by third parties. Some of these third parties may include contractors, vendors, or other individuals

that have access to the company's property or assets including orchestrating a kickback scheme with an insured employee.

## PARTIES AND EXPERTS INVOLVED IN A FIDELITY CLAIMS INVESTIGATION

Fidelity claims typically include several parties, the most obvious being the insured or policyholder and the insuring party or insurance carrier. However, due to the nature of the fidelity claim, other parties are involved in the claim process, and each party has a distinct role they play in the process:

- **Insured / Policyholder:** The policyholder is the individual or business that is identified in the fidelity insurance policy as the covered party. Once fraudulent activities or dishonest actions have been detected and identified, the policyholder submits a claim for the covered loss to their fidelity insurance carrier in the form of a notarized Proof of Loss. This Proof of Loss should include a narrative description of the loss particulars (schemes), specific coverages that the insured feels respond to the claim, date of discovery, theft agents, period covered by the loss, support for all aspects of the loss, and the total amount of the claim. Depending on the size of the policyholder organization, they may have an internal audit or risk control department involved in uncovering and documenting any employee fraud.
- **Insurance Carrier / Insurer:** The insurance company's claims handling team is responsible for ultimately assessing and processing claims made by the policyholder. Once a claim is filed, the insurer determines whether the claim is covered, what portion of the claim has been properly supported and quantified, and how much the insured is owed in satisfaction of their claim. As part of the claim review process, the insurer may involve the policy holder, underwriter, inside counsel, outside counsel, internal or external forensic accountants, information technology (IT) experts and others that can bring clarity to any major claims issue.

- **Insurance broker:** The insurance broker is typically the individual that acts as the intermediary between the insurance company and the insured. Through their service, the insurance broker understands the background and needs of the insured to assist them in selecting an insurance policy that best fits their situation and actively works to obtain the best coverages at the most affordable rate for each policyholder.
- **Alleged Dishonest Employee or Third Party:** Depending on the circumstances of the claim, there is either an alleged employee(s) or third party that perpetrated dishonest or fraudulent acts that resulted in financial losses. These theft agents may engage their own counsel in defense of the allegations made against them.
- **Law Enforcement:** When submitting an employee dishonesty claim, many fidelity policies require the policyholder to file a criminal complaint against the alleged dishonest employee and cooperate with law enforcement. In these situations, law enforcement often become involved in the investigation and gathering of evidence for potential criminal charges. It's not unusual for a theft claim to run parallel on two fronts, a civil and a criminal investigation. It's important for the financial investigation team to develop a rapport with the criminal investigators and to aid one another as much as is legally allowed, to gain as full an understanding of the schemes and actions perpetrated by the theft agent.
- **Claims Adjusters:** On behalf of the insurance company, the claims adjusters investigate and evaluate the fidelity insurance claims. It's quite common for fidelity claim examiners to come from a legal background, many with legal designations. They review the policy, gather and analyze the evidence, determine the extent of the covered loss, and often recommend retaining additional experts and professionals to assist in the claims review process. These professionals can include attorneys, forensic accountants, IT, equipment, and other claim-specific experts.
- **Legal Counsel:** In complex fidelity claims, various parties may hire legal counsel to represent their interests. Often, the insurance company, policyholder, and possibly the alleged dishonest employee or third party will retain legal counsel who provides guidance throughout the claims process and may assist in negotiations or resulting litigation.
- **Forensic Accountant:** Insurance companies usually have their own internal claims accounting groups who routinely assist various claims adjusters in understanding the financial aspects of different claims. Fidelity claims frequently involve financial malfeasance and, depending upon the circumstances, claims adjusters and insurers may choose to hire independent forensic accountants to help gather and analyze the evidence, evaluate the validity of different aspects of the claim, and quantify the extent of supported losses for the carrier. This then allows the carrier to apply coverage and determine the amount of covered loss per the insured's fidelity policy.
- **Other Experts:**
  - o **Digital Forensics:** Digital forensics professionals are required to gather information in a secure manner from email systems, mobile devices, databases, file shares, general ledger systems, etc. The data gathered may be used in legal proceedings, especially if referrals to law enforcement are contemplated. As a result, it is important to document collection records, chain of custody, and perform ESI (electronically stored information) data capture in accordance with industry standard forensic preservation practices. In addition to the data preservation efforts, additional technical experts may be necessary to assist with document review capabilities, database analytics, and reporting of the information relevant to the investigation.
  - o **Global Investigations:** Successful subrogation recovery may depend upon the global scope and outreach available from your claims recovery team. Identification of potential recoverable assets in foreign countries requires local expertise as to the laws and regulations governing the recovery of ill-gotten funds.
  - o **eDiscovery:** eDiscovery professionals are required to process, search, and facilitate the review of unstructured data (such as electronic

communications like email and text messages). These tools allow for the application of advanced search techniques that provide investigators with the ability to deploy artificial intelligence to identify potentially relevant documents discussing the fraud. This is especially effective in situations where the alleged dishonest employee(s) used codewords when discussing the fraudulent activity.

- o **Data Analytics:** Investigative data analytics professionals review and analyze financial systems that may have transaction level details associated with the alleged fraud. By reviewing and reporting on the transactions that are subject to the investigation, the data analytics professionals can help to quantify the scope of the potential loss. Additionally, by applying ongoing risk assessment techniques to the financial systems, new automated compliance procedures can add to standard review processes to potentially limit future exposure to these issues.
- o **Asset Search and Recovery Group:** A key component to your subrogation recovery efforts is a thorough asset search to include the names and locations of all known (and yet unknown) associates of the theft agent. An experienced asset search team can aid the insurer in identifying potential assets for seizure / forfeiture and direct law enforcement toward capital that can potentially be frozen while the investigation is ongoing. These professionals utilize public information sources such as news articles, social media posts, and other public disclosures to target investigation efforts. Relatives, bank accounts, assets owned, travel frequencies, phone records, identification numbers, former employers, investment accounts, tax returns, insurance policies, bank activity, disbursement history and the like allow the recovery group to build a financial history that can lead to a maximization of any available recovery.

## NAVIGATING CLAIMS CHALLENGES & HOW EXPERTS CAN HELP

Throughout the claims handling process, issues or challenges may arise for which parties involved must reconcile. Here are some common issues that may be encountered:

- **Proof of Loss:** One of the primary challenges in fidelity claims is establishing the proof of loss. The insured party must provide evidence of the fraudulent or dishonest acts committed by an employee or third party. Evidence may include financial records, transaction logs, emails, banking records, internal investigation reports, witness statements or interviews, criminal or civil litigation against parties of interest, or other documentation. Gathering the electronic evidence may require digital forensics professionals to ensure the data is preserved in a defensible way. eDiscovery review tools can also be useful to facilitate the review of this evidence so that it can be presented to the insurer as evidence of the loss. Proofs of Loss may require time for the policy holder to compile and properly document as frauds, by their very nature, are hidden and therefore require the insured / investigator to “peel back the onion” in order to get to the root of the theft scheme.
- **Policy Coverage:** Understanding the specific coverage outlined in the policyholder’s fidelity policy is a crucial step of the claims process. Policies vary in terms, conditions, and coverage / sublimits across different types of organizations. Therefore, the parties must ensure that the claim falls within the scope of the policy, understand the policy limits, and whether the insured is allowed to stack available policy limits. Policies may require the insured to demonstrate that the employee received an improper financial benefit from their actions.

For employee dishonesty or fraud claims, another issue is often the verification of employment status and whether acts by that employee are covered. Most fidelity policies define the term employee and who is covered or excluded, such as regular employees of the insured organization, 1099 employees, owner (normally excluded from coverage), named insured,

or uninsured subsidiary. Additionally, most policies outline a number of specific exclusions, including if the insured knew about prior fraudulent activity by that employee.

- **Policy Exclusions:** Fidelity policies often contain exclusions that specify certain individuals, situations, or types of losses that are not covered. The insurance company, claims adjusters, and other professionals need to review these exclusions at the onset of the claim investigation to understand how they may apply to the claim and to ensure that the investigation addresses each potential exclusion. Other typical exclusions include indirect or consequential losses, such as impacted credit rating, loss of potential income, and fines or penalties.
- **Reporting Timelines:** Issues may arise over when the insured discovered and reported the fraudulent or dishonest act. Fidelity insurance policies typically require the insured to report the act promptly, and failure to report within the specified timeframe could result in the insurance company denying the claim. Exactly when the insured first determines when a possible employee theft has taken place is often an area for potential debate between the carrier and insured. The financial investigator must be cognizant of the date of discovery issue and obtain relevant information to help the insured make the date of discovery determination. Metadata associated with key electronic files can help to determine the exact time associated with fraudulent or dishonest activity.
- **Investigation:** Insurance companies may conduct their own investigation of the claim to assess the validity of the claim. However, for more complex claims, outside forensic accountants are often hired to examine the claim, both by the insured and the insurer. These independent professionals evaluate the circumstances and evidence surrounding the loss, identify the responsible parties, conduct interviews of key personnel or parties, and quantify the loss amounts. For some claims, the forensic accountants should be able to provide expertise in the location and possible recovery of stolen assets, such as money, inventory or other physical assets purchased with stolen funds. Also, forensic accountants or investigators with specific expertise or language skills may be needed, particularly if assets have been diverted to foreign countries. Digital forensics and data analytics experts can assist with analysis of financial systems, alternative asset categories (such as crypto currencies), and asset tracing activities.
- **Subrogation:** If the insurance company pays a claim to the policyholder, the insurer often seeks to recover its losses through subrogation: usually through legal proceedings. During this process, the forensic accountant, legal counsel, and other professionals can assist in the proceedings with guidance as to the nature and location of hidden assets and possibly provide expert witness testimony against the fraudsters.
- **Mitigation of Loss:** The fidelity insurance company often requires the insured to take reasonable steps to mitigate any future losses, once the fraudulent or dishonest activity is discovered. Forensic accountants and other professionals can assist in evaluating the organization's current internal controls and providing recommendations. Insureds are often asked to provide their carriers with any changes they make to their internal control (I/C) systems in response to the theft. Evaluations of these I/C changes allow the carrier to make a determination about whether or not to provide continuing fidelity coverage for the insured.
- **Documentation:** As with any investigation, thoroughly documenting the fraudulent or dishonest acts is crucial to a successful claim. All parties involved, especially the claims adjusters, investigators, and forensic accountants, should ensure the preservation of evidence to avoid spoliation, maintain a clear chain of custody, and the successful organization and analysis of large data and document sets. Digital forensic and electronic discovery professionals can work with the investigators to gather, preserve, and analyze the documents and process large volumes of information which sometimes seem overwhelming. Key word searches allow the investigator to zero in on the most relevant data to enable the insured and carrier to ascertain the magnitude of the defalcation and the viability of the supporting data.
- **Dispute Resolution:** In certain cases, disagreements may arise between the insured and the insurance company regarding the claim's validity, or the amount

covered. When this occurs, the dispute may need to be resolved through various dispute resolution methods, such as negotiation, mediation, arbitration, or legal proceedings. Throughout this process, legal and accounting professionals can assist in the dispute resolution process to aid in a successful outcome. With this in mind, the forensic investigator should maintain their file with an eye towards possible litigation, making their file litigation ready before litigation is ever contemplated. Using a document tracking system that links key documents to reports and analysis helps achieve this goal.

## ADDITIONAL EXPERTISE THAT MAY BE NEEDED IN A FIDELITY INVESTIGATION

Depending on the insured's industry, or the types of information requiring analysis, specific technical expertise may be required to address the investigation's needs.

- **Cryptocurrency:** Cryptocurrency has been used more and more by threat actors as a way to not only hide their identity, but also limit visibility into the flow of value as it changes hands on the global blockchain. Deploying skills to quantify and trace assets on a chain can be critical to a company's ability to recover lost assets through fraudulent means.
- **Electronic Device Forensics:** Digital forensics experts may need to dig deeper into specific device classes to identify additional communication platforms. For example, documents and data that have been deleted may need to be recovered to aid the investigation. Additionally, encrypted messaging apps (like Signal, WhatsApp, and Telegram) may not be immediately evident when reviewing collected electronic evidence. Forensics experts can evaluate the data sources using a variety of forensic tools to determine if specific apps are present and how to access the communications they contain.
- **Cyber:** On many occasions, the security architecture of a company plays a key role in how sensitive information becomes available to a threat actor. Poor security protocols and data storage standards provide

opportunities for fraudulent activity and information misuse outside of typical data governance models and deployed checks and balances. For example, if an employee that shouldn't have access to approve vendor invoices finds a way to access the general ledger and purchasing systems, it could be possible for them to gain enough information to create a fake entity that could circumvent compliance efforts. It's important to compartmentalize access to specific areas of the business and regularly audit that access to ensure that security breaches don't occur.

- **Industry Specialists:** If the insured is situated within a highly regulated industry (such as securities, healthcare, public sector, etc.) specialists that are familiar with the datatypes as well as the regulations and compliance standards of the client can be invaluable at limiting the scope of the investigation and applying focus to the specific transactions at issue. Knowing the compliance procedures that the insured is undergoing on a regular basis can help to streamline what areas to focus an investigation on and to highlight areas in the shadows of the regulators. Furthermore, these industry experts can assist with implementing process improvements to help limit these types of activities in the future.

## TYPES OF FIDELITY POLICY EXCLUSIONS

There are typically a host of exclusions that appear in most fidelity policies. Coverage that seems to be granted within the declaration pages, loss determination pages or endorsements are often clarified within the *Exclusions* sections of the policy. It is vitally important for the investigation team to have a thorough understanding of the entire insurance policy, with a watchful eye toward the exclusions section. All coverage determinations are the exclusive purview of the insurance carrier and their counsel. The insured and their counsel may well have a different interpretation of certain aspects of the policy, but in either case, the forensic accountant's role is to understand the key aspects of the policy, including afforded coverages and related exclusions. However, under no circumstances is the forensic investigator to make any coverage determinations. All questions regarding coverage must be deferred to counsel / carrier.

Some typical exclusions that we often find in fidelity bond coverages are:

- Limitations on which afforded coverages apply to employees
- Exclusions for acts of Owners, Partners, Directors of the insured
- Losses that take place after the discovery of the employee theft
- Consequential losses
- Cost to establish the theft loss unless provided as noted coverage
- Loss of potential income or dividends
- Any damages other than direct compensatory
- Losses dependent solely upon a physical inventory or Profit and loss computation
- Accounting errors.

## CONCLUSION: ADAPTING FIDELITY CLAIMS TO A CHANGING LANDSCAPE

Every fidelity claim is unique and different, but they all need a qualified, experienced group of professionals to address the various aspects of each claim. Finding experts who work hand-in-hand with one another to address the unique challenges of each specific claim is critical to achieving the best outcome.

At the same time, the future of insurance is highly dynamic and can be influenced by unexpected events, changes in business practices, emerging risks, and emerging technologies. For example, since ChatGPT emerged in late 2022, we have already seen an impact in how fraud is being conducted as well as investigated with this new generative AI technology. As a result, fidelity insurance providers will continue to adapt to the changing landscape to remain effective in managing and processing claims. In turn, businesses need to also stay informed about these changes to mitigate losses, prevent losses from occurring, and ensure adequate coverage for their specific risks.

## ACKNOWLEDGMENTS

We would like to thank Peter Fogarty, CPA, CFE, CFF, Natalie Lewis, CPA, CFF, CFE, and Stephen O'Malley for providing insights and expertise that greatly assisted this research.

[Peter Fogarty](#) is an Executive Vice President in J.S. Held's [Forensic Accounting practice](#). He has more than 35 years of expertise in forensic accounting and fraud examination. As a Certified Public Accountant and Certified Fraud Examiner, who is also certified in financial forensics, Peter specializes in the financial evaluation of damage claims and frauds, including first-party property losses, third-party liability cases, commercial litigation damages, and fidelity matters. He has significant experience assessing damages for both domestic and international organizations, including many Fortune 500 companies. In addition, he has managed several nationwide catastrophe response programs and has been responsible for the forensic accounting analysis of claimed damages exceeding \$400 million. He has litigation experience in various courts throughout New England and has testified in both state and federal courts in cases involving such matters as commercial loss of income, contract disputes, fraud, personal injury, and subrogation.

Peter can be reached at [pfogarty@jsheld.com](mailto:pfogarty@jsheld.com) or +1 401-741-9944.

[Natalie Lewis](#) is a Senior Vice President in J.S. Held's [Economic Damages & Valuations practice](#). As a Certified Public Accountant and Certified Fraud Examiner, who is also certified in financial forensics, Natalie specializes in forensic accounting and the analysis of economic damages. She provides consulting and expert services for both plaintiff and defense law firms throughout the country. Natalie has conducted fraud investigations for companies of all sizes as well as government entities. Her investigations have spanned the globe and include various internal investigations, embezzlement, Ponzi schemes, commercial crime insurance claims, Foreign Corrupt Practices Act (FCPA), and asset misappropriation.

Natalie can be reached at [natalie.lewis@jsheld.com](mailto:natalie.lewis@jsheld.com) or +1 470 852 4601.

[Stephen O'Malley](#) is a Senior Managing Director and leads [Digital Investigations & Discovery](#) services within J.S. Held's [Global Investigations practice](#). He has been



engaged on some of the largest multinational investigations and has given expert testimony in the areas of analysis and restoration of electronic data, electronic discovery best practices, and testing of related computer software. He is an expert eDiscovery practitioner and data analyst. Stephen has significant experience in major fraud and corruption investigations including FCPA, Ponzi schemes, U.S. Department of Justice and SEC investigations; in multijurisdictional litigations; in provision of evidence for litigation support; and in advanced data analysis.

Stephen can be reached at [somalley@jsheld.com](mailto:somalley@jsheld.com) or +1 718 510 5617.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.