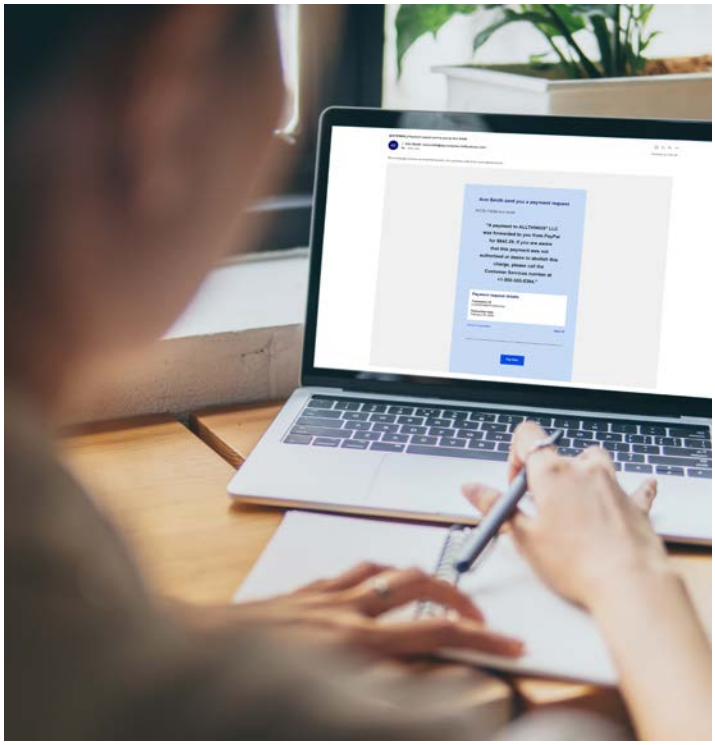
North America Financial Lines: Crime Insurance & Fidelity Bonds

This edition of AIG's Claims Intelligence Series focuses on loss trends in U.S. crime insurance and fidelity bonds, as well as best practices to help mitigate the frequency and severity of these losses. This report includes AIG claims data on nearly 700 paid crime and fidelity matters noticed to U.S. Financial Lines policies between 2020 and 2022.

The most mature of the Financial Lines products, crime insurance and fidelity bonds rarely experience major disruptions or changes in claims trends. However, an analysis of AIG claims data reveals that this paradigm has been upended in recent years by the proliferation of social engineering fraud, also known as impersonation fraud. A seemingly endless pool of targets coupled with high success rates is fueling an evolution of fraud schemes aided by ever-changing technology that is adding a material new source of crime and fidelity loss.

At the same time, the data affirms that small and midsize organizations are disproportionally burdened with crime and fidelity losses, falling victim more frequently than their larger counterparts.



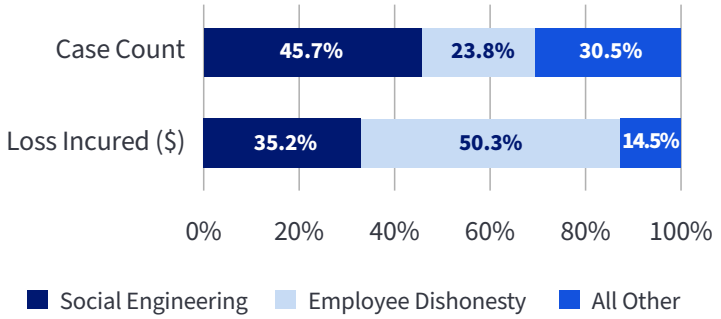
At a glance

- Social engineering fraud, or losses due to schemes duping an employee into transferring funds, are a significant and growing threat for companies of all sizes.
- Small and midsize organizations are particularly vulnerable to all types of crime and fidelity losses.
- Service-focused enterprises are the most frequent targets of crime and fidelity events. They typically have multiple revenue streams, which makes identifying red flags and quantifying losses more difficult.
- Crime Insurance addresses loss of money, securities, and other assets resulting from dishonesty, theft, or fraud for commercial and governmental entities.
- Financial Institution Bonds provide financial institutions and financial services firms with tailored protection from employee dishonesty, theft on premises, forgery, computer systems fraud, impersonation fraud, and a variety of other risks.

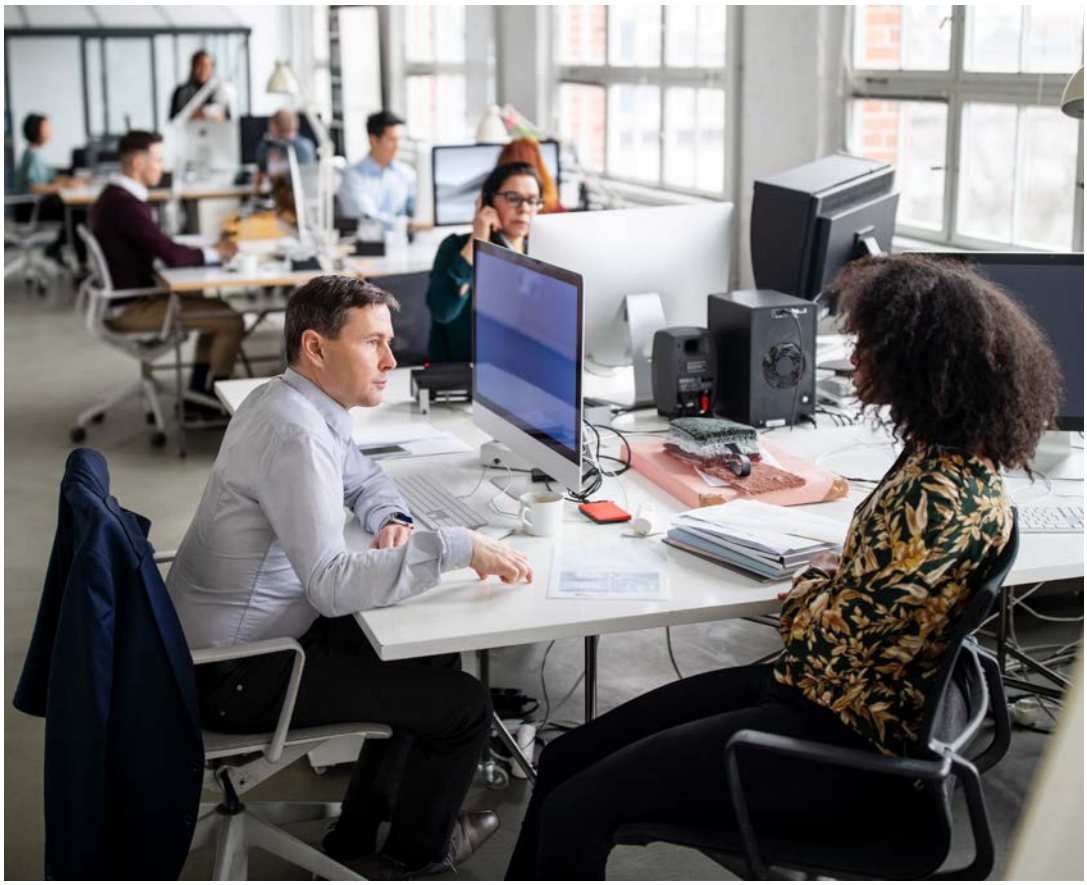
The Universe of Threats

Social engineering fraud, defined as loss connected to schemes duping an employee to transfer funds, began to emerge as an exposure in the mid-2010's. Initially, the exposure resulted in few claims and limited loss, but over time the frequency and severity of social engineering fraud claims has grown exponentially. The exposure now accounts for nearly half of claims reported and more than one third of losses incurred during the time period studied. Absent diligent underwriting of social engineering fraud exposures and the application of sub-limits to the coverage, these losses would be an even larger percentage of overall insured losses.

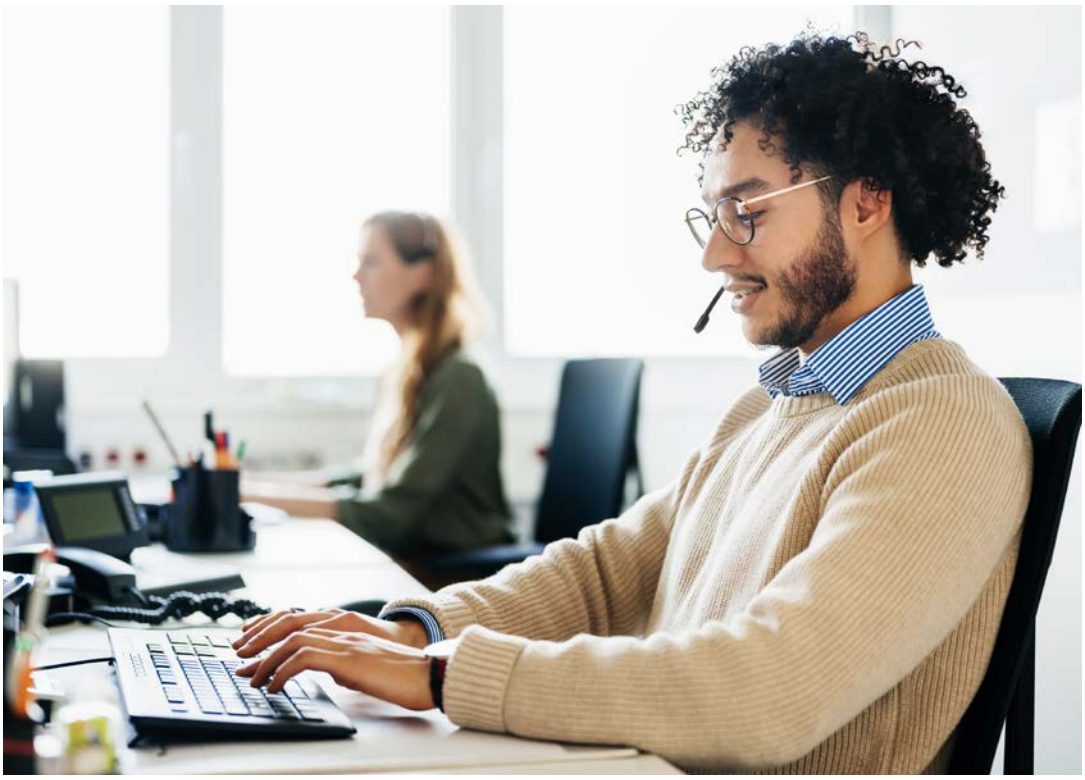
Crime and Fidelity Claims Makeup



Employee dishonesty, which encompasses a broad spectrum of employee theft and fraud schemes, was previously the most frequent source of loss, but it now ranks second behind social engineering fraud, accounting for slightly more than 23% of claims.



Employee dishonesty accounted for nearly one in four claims reported.



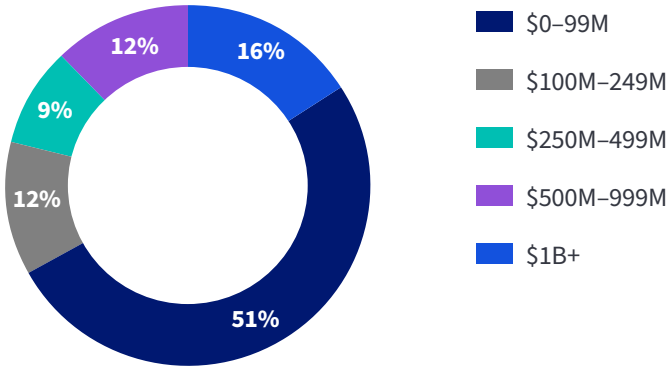
The frequency of social engineering fraud and employee theft claims is materially higher for small and midsize organizations, which typically have less sophisticated risk management resources.

Small & Midsize Organizations Facing Higher Claim Frequency

We examined claims data from multiple angles, including the size of the organization, the size of the claim, and industry sectors most impacted. In each case, the data shows that a preponderance of claims fall on small and midsize organizations.

Claims by Company Revenue Band

- More than 50% of claims impacted organizations with less than $99 million in revenue.
- 84% were incurred by organizations with revenues less than $1 billion.



Insureds with less than $99 million in revenue accounted for over half of the claims in the study period. These smaller organizations are more likely to have limited risk management resources and investment in internal controls. Their exposure also tends to increase by trusting key employees with start-to-finish authority over financial transactions, rather than following best practices to separate duties.

At the same time, smaller organizations are particularly stretched by the current challenges common among their industries. This includes the need to adapt to customer demands and instill strong internal controls as remote work transforms the landscapes, while labor shortages and economic pressure leave resources thin. Perpetrators are capitalizing on these challenges.

Impacts by Industry Sector

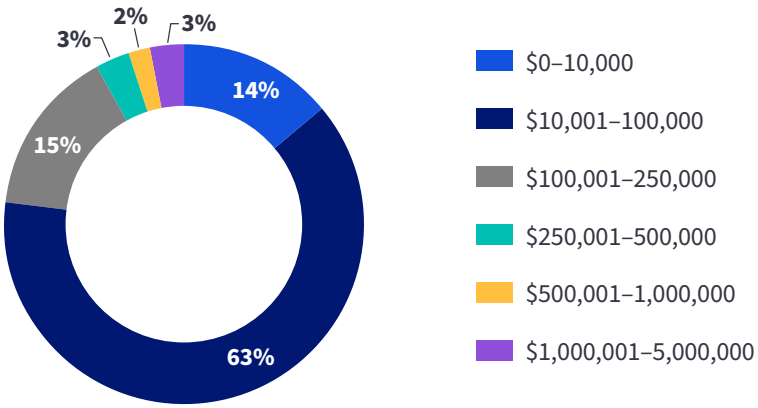
Educational service providers, government entities, and membership organizations/associations experience the highest frequency of claims.

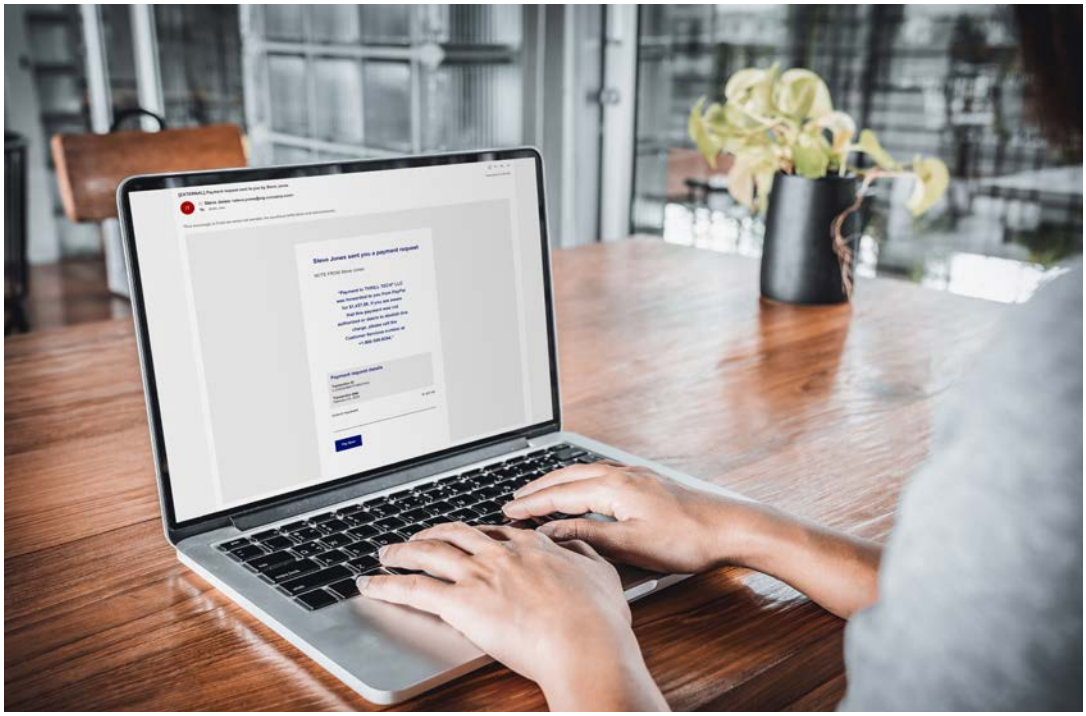
These sectors tend to be service focused and have frequent transactions and diverse revenue streams that can be difficult to track. They typically operate on tight budgets with limited risk management funding and staffing, oversight, and dual-control options. In addition, these institutions usually have easily transferred assets, routine small balance transfers, and high staff turnover, which can all contribute to loss frequency.

Loss Size

The majority of claims during the period studied had a loss amount less than $100,000. These claims are more likely to come from small to midsize organizations that generally have smaller amounts of transferable assets.

Claims by Size





Insuring Social Engineering Fraud Risk

The Fidelity Research & Investigative Settlement Clause: Improving Loss Resolution

AIG's Fidelity Research & Investigative Settlement Clause (FRISC) offers a streamlined way to investigate and settle losses, which may be advantageous for small and midsize organizations.

By electing FRISC, an insured can initiate investigation and evaluation of a claim by an independent third party – with both the insurer and the insured agreeing to abide by the conclusions. As a result, FRISC provides access to an expedited, cost-efficient, and effective claim evaluation and resolution process. It also enables small and midsize organizations to more quicky establish the nature and extent of the control weakness that allowed the incident, so they can more quickly remedy it and reduce the likelihood of future loss.

Results

- **Efficient claim evaluation**
- **Reduced back-and-forth**
- **Expedited adjustment process**
- **Reduced investigative costs**

Despite increased awareness, expanded fraud training options, and diligent underwriting that helps to identify inadequate controls, social engineering fraud remains a major loss driver.

With thorough underwriting and confirmation of best practice controls, we expect that carriers will continue to make essential protection available, providing higher limit options and broader coverage for the exposure. Limits offered will vary, and it is likely that larger sub-limits will be more readily provided for financial institutions rather than commercial accounts.

In many cases, a social engineering fraud claim triggers a corresponding security failure or privacy event claim under a cyber policy. When multiple fraud schemes are involved, a comprehensive management liability insurance solution is critical.

Five Tips for Better Loss Prevention

The following best practice recommendations are foundational and designed to help prevent or mitigate crime and fidelity losses. Demonstrating implementation and consistent use of best practices may also help insureds secure coverage for social engineering fraud at more favorable terms and conditions.

1. Require multiple parties to approve funds transfers and changes to payment or deposit account details. **Eliminating unilateral authority immediately complicates fraud attempts and improves process confirmation.**
2. Ensure dual-control procedures/separation of duties in accounts payable functions. **Regularly audit these functions to ensure adherence.**
3. Continually invest in IT security advancements to help filter, prevent, and flag phishing attacks and spoofed emails. **Robust IT security complements internal controls by identifying and intercepting fraudulent messages.**
4. Regularly review access credentials and require frequent password changes. **This improves overall security and limits access for separated employees and contractors.**
5. Continually communicate, audit, and enforce adherence with internal controls and policies. **Implementing best-in-class controls is essential; ensuring adherence, without employee "workarounds," is even more so.**

While FRISC is a benefit for all insureds, its advantages are amplified for small and mid-sized organizations with limited risk management resources.

Case Studies

The insured received a fraudulent email requesting a change in the bank account details of an existing construction vendor. The insured's employee made the change and wired a $300,000 invoice payment to the new bank account. When the vendor informed the insured that funds were not received, the insured realized that the money was wired to a fraudulent account. The AIG claims adjuster worked in close contact with the insured throughout the course of the claim evaluation to ensure a smooth, efficient resolution and payment for this covered loss.

A management employee of a medical center colluded with a vendor representative to bill the insured close to $4 million for surgical implants, which the insured later discovered were not used for surgeries. The employee manipulated records to conceal the fraud and took advantage of the lack of coordination between handwritten records and the electronic record system. An independent third-party firm was engaged via FRISC, and the total amount of this complex loss was determined promptly, allowing for a swift resolution and payment.

A municipal employee fraudulently used his corporate purchasing card to buy $1.4 million in printing toner that he transported to his home to resell online. He also used his corporate card to make $21,000 in fraudulent personal purchases from online retailers. The fraud went on for several years before being discovered. Once the extent of the loss was determined and executed proof of loss submitted, the full policy limit of $1 million was paid.

AIG insurers are a leading provider of Crime Insurance and Fidelity Bonds for commercial organizations and financial institutions of all sizes. We have long specialized in bringing these vital solutions to small and midsize organizations. Our crime and fidelity underwriters, who average more than two decades of experience, tailor coverage for each client's unique needs. Our dedicated claims team and our underwriters continually track emerging loss trends and partner with insureds to ensure coverage and controls continually outpace evolving risks.

For more information, please contact:

Jessica Cafarelli
Head of First Party Products
North America Financial Lines
T: 646-565-7906
jessica.cafarelli@aig.com

John Patterson
Head of Financial Institutions,
Fidelity, and M&A Claims
T: 646-477-2449
john.patterson@aig.com

AIG

www.aig.com