# 2024 Fidelity and Crime Insurance

## Market Outlook

Fidelity and crime insurance provides financial protection for losses businesses could face due to fraudulent acts by their employees or third parties. Covered events may include credit card forgery, computer fraud, and theft or destruction of property. The fidelity and crime insurance segment has seen mostly favorable conditions in recent years, primarily due to new entrants generating increased market competition. As a result, most policyholders have experienced flat to modest rate increases and sufficient capacity.

However, several market trends could impact claims and related costs throughout the fidelity and crime insurance space in the coming year, including a surge in social engineering fraud (SEF) incidents and rising concerns regarding coverage for digital intangible assets. Going into 2024, industry experts anticipate that the majority of insureds will encounter flat premiums, while those lacking proper loss control measures could be more susceptible to rate increases and coverage restrictions.

## Developments and Trends to Watch

- **Greater market competition—**The last few years have fostered considerable growth in the fidelity and crime insurance segment, evidenced by new entrants and an increasingly competitive market. Specifically, a rising number of insurance carriers—namely, those who historically operated within the professional and management liability markets—have emerged in the segment as a way to diversify their portfolios, enhance their coverage offerings and enter a line of business that has demonstrated more profit potential than others. In response to these shifting market dynamics, most policyholders (especially small and midsized businesses) have benefited from a competitive pricing landscape, thus limiting the likelihood of large-scale rate increases. Yet, it's worth noting that insureds with complex risks may still face premium jumps and coverage limitations.
- **SEF challenges—**SEF refers to a scamming technique in which a perpetrator preys on key human behaviors (e.g., trust of authority, fear of conflict and promise of rewards) to obtain unwarranted access to a target's technology, funds or data. These incidents have driven up the frequency of low-severity loss activity in the fidelity and crime insurance space. Complicating matters, carriers in the segment have adopted limited risk appetites for SEF incidents; according to recent research, many carriers provide sub-limited coverage for these incidents, with average limits falling below $500,000 and solely applying to the "direct theft" of funds. This means that the nature of SEF events and related losses (e.g., theft or destruction of property) are often subject to coverage exclusions, leaving businesses with significant out-of-pocket expenses. While businesses may seek additional protection for SEF incidents through cyber insurance policies, such coverage also comes with various exclusions. As such, some companies have purchased specialized policy endorsements or standalone coverage (e.g., social engineering insurance) to ensure proper protection for SEF events.
- **Digital intangible asset concerns—**Over the past couple of years, many businesses have acquired digital intangible assets, including cryptocurrency, blockchain and nonfungible tokens. In light of this trend, questions have emerged regarding how fidelity and crime insurance will respond to the theft or destruction of such assets. As it stands, the unknowns and evolving risks surrounding these assets have caused many carriers to be hesitant to provide coverage, even in instances where minimal exposures are present. Therefore, to maintain transparency and reduce the risk of coverage ambiguity, some carriers have adjusted their policy wording to clearly exclude losses associated with digital intangible assets. With this in mind, it has become all the more critical for businesses with these assets to prioritize effective risk management strategies.

## Tips for Insurance Buyers

- Adopt a strong security culture. This may entail implementing policies that promote adequate oversight of company assets and limit access to these assets.
- Utilize in-depth vetting protocols (e.g., interviews, character assessments, professional references and background checks) amid the hiring process. Be sure to spread out asset-handling duties among your staff and educate all employees on prevalent security topics and potential theft indicators.
- Consult insurance professionals to review your fidelity and crime exposures and secure proper coverage.

WINTERS-OLIVER
INSURANCE AGENCY, INC.