Crime Market Update: (Q3) 2022

State of the Market

- The Crime market is firming largely due to pandemic, remote work environment and a related increase in cybercrime.
- In 2021, Americans were hit by an unprecedented rise in cybercrime, with nearly 850,000 reports to the FBI and losses surpassing $6.9 billion.
- Q3 Premium increases can be expected in the range of 5-10% depending on loss history. Organizations that have experienced losses should expect more significant premium increases.

Legal & Regulatory Developments

- The Internet Crime Complaint Center (IC3) has received 440,000 complaints per year with $13.3 Billion in losses over the last five years. With many current claims relating to CARES Act Fraud (grant fraud/loan fraud/and Phishing fraud).
- Increase in claims of Social Engineering Fraud and Invoice Manipulation Fraud/Vendor-Client Fraud.
- Courts continue to grapple with the interplay between computer fraud coverage, sitting within a Crime policy, and computer hacking-related coverage that exists in a Cyber policy.
- On May 6, 2022, President Biden signed the *Better Cybercrime Metrics Act* (BCMA) into law, in response to increasing public concern about cybercrime and the lack of comprehensive cybercrime data and monitoring in the United States.

Coverage Trends: Pricing, Terms & Conditions

- Insurers continue to seek premium and retention increase.
- Capacity remains stable but more complex risks with crypto exposure could have issues securing primary and low excess capacity.
- Social Engineering Limits are being reduced and market are reluctant to provide high limits to new buyers.
- Overlapping coverage between Crime and Cyber policies is becoming more of a focus and is causing more claims/coverage-related issues. Privacy/Cyber Related Exclusions are becoming standard.
- Underwriters are requiring much more detail on applications; specifically relating to funds transfer controls, wire transfer controls, vendors and client controls.
- Companies with international crime exposure remain very hard to place due to high exposure for embezzlement and vendor fraud.

Emerging Risks & Trouble Spots

- Fraud has been on the rise, in part, due to Pandemic imposed remote-work environments. This is expected to continue as many fraudulent schemes can take 18-24 month to uncover. In addition, the remote work environment (or at minimum a hybrid work environment) appears to be something that will remain with many organizations going forward.
- High inflation and the threat of recession means the market is likely to see an increase in various types of Occupational Fraud, specifically Employee Theft.