Claims arising from social engineering losses have increased significantly in recent years. Law firms, title agents and other professionals are frequent targets of bad actors seeking to divert funds through schemes that trick insureds into believing they are wiring funds to intended recipients. Once funds are transmitted by the insured to the wrong account, it can be incredibly difficult to stop or recover payments from the financial institutions that facilitate the payment. And clawing back the funds from the bad actor is virtually impossible.

This scenario often leads to significant claims from third parties against insured companies for allowing bad actors to infiltrate their network or failing to confirm payment details. Losses from these events can be crippling, especially to small to mid-size companies. Policyholders and their brokers often overlook this risk when purchasing insurance. Although there are specific cyber and crime policies that afford coverage for these losses, insureds sometimes believe they are able to rely on their standard E&O policies to cover these claims. A recent decision from the Illinois Appellate Court further dispels that notion. The decision also provides helpful guidance on when an insurer can consider extrinsic evidence in denying a duty to defend.

In *Certain Underwriters at Lloyd's v. Galey Consulting, LLC*, the First District Illinois Appellate Court held an insured's summary to its insurer notifying it of a potential claim stemming from an incident of e-mail hacking and wire fraud was properly considered when determining whether an E&O policy's cyber events exclusion precluded coverage, despite the lack of mention of the cyber-attack in the underlying complaint.

Monroe Infrastructure Inc. was engaged in a project for infrastructural improvements in Tennessee. Monroe then engaged the services of Galey Consulting to provide professional construction management services. In pertinent part, Galey Consulting was responsible for reviewing and approving requests by subcontractors and others to receive payment by Monroe for work done on the project.

On March 23, 2022, an agent of Galey gave notice to Underwriters of an incident which had the potential to give rise to a claim under their policy, which included a summary of events from Galey detailing the incident. The incident stemmed from a cyber-attack, in which hackers gained access to Brian Galey's email, and diverted emails from Nashville Electric Service ("NES") so Galey would not receive them. From there, the hackers sent Galey a fraudulent email purportedly from NES notifying him that their payment procedures changed such that checks would no longer be accepted, and electronic funds transfers would be required. Galey ultimately directed Monroe to make a payment of $673,384.18 to a fraudulent bank account via wire transfer.

Underwriters issued their coverage position, stating that the policy did not carry any cyber or privacy coverage for the incident, nor did the errors and omissions policy apply. Monroe sent a reimbursement demand to Galey, and Underwriters subsequently filed an insurance coverage action seeking a declaratory judgment that no coverage was available under the policy for the reimbursement demand pursuant to a cyber event exclusion.

Monroe then filed a lawsuit against Galey, seeking to recover the $673,384.17 that was sent to the fraudulent bank account. Monroe's complaint did not allege that an e-mail or wire fraud incident played any role in causing the loss suffered. Monroe's complaint sought recovery under

three theories of liability: professional negligence, errors and omissions; breach of contract; and breach of fiduciary duty. Underwriters then amended its complaint for declaratory judgment to include greater detail than the initial complaint, but its material allegations remained that it was clear from Galey's initial summary of events that Monroe' demand for reimbursement and underlying lawsuit arose out of an event of e-mail hacking and wire fraud such that coverage was not available under the policy pursuant to the cyber event exclusion. The trial court granted Underwriters' motion for summary judgment, finding that Underwriters had no duty to defend Galey Consulting or Brian Galey in the underlying lawsuit, nor did Underwriters have a duty to indemnify Monroe with regard to the consent judgment.

On appeal, Monroe argued that the duty to defend analysis could not include consideration of Brian Galey's summary of the cyber-attack provided to Underwriters. Monroe argued that Underwriters' duty to defend Galey Consulting and Brian Galey in the underlying case must be determined exclusively by comparing the allegations of the underlying complaint against the terms of the policy. The appellate court found that there may be circumstances in which courts may appropriately look beyond the allegations of the complaint to determine whether an insurer has a duty to defend, and Brian Galey's summary fell within such circumstances. The court noted that it was clear the alleged loss stemmed entirely from the cyber-attack on Galey. The court further stated that the absence of allegations regarding the cyber-attack, when it was the root cause of the loss, does not require the court to wear judicial blinders to the role that an e-mail hacking incident played in causing the loss when determining the applicability of an exclusion.

Monroe's second argument was that, even if Brian Galey's summary was considered, the policy's cyber events exclusion did not preclude coverage for losses that have other concurrent causes; Monroe asserted that the cyber events exclusion did not bar coverage because the allegations attributed the loss to various acts, errors, omissions, and misrepresentations by Galey. Monroe argued the language of the exclusion constituted a limited causation model for determining whether or not the exclusion applied meaning that, for the exclusion to apply, the loss in question must 'arise' out of the defined 'cyber event.'

The appellate court rejected Monroe's argument that any acts or omissions alleged in the underlying complaint are concurrent causes of its loss, such that its loss cannot be characterized as "arising directly or indirectly out of any cyber event." The court noted that the Illinois Supreme Court has held the phrase "arising out of" has a set meaning in law, which is defined broadly and refers to a causal connection. The appellate court found it clear from Brian Galey's summary of events that Monroe's loss can only be characterized as arising directly or indirectly out of a cyber event, even if other potential causes of the loss can also be identified.

As such, the appellate court affirmed the trial court's judgment, holding that the summary Galey provided his insurer describing the e-mail hacking and wire fraud was properly considered in the duty to defend analysis, and summary judgment in favor of Underwriters was appropriate.

The court's decision highlights the importance of purchasing insurance that covers these types of social engineering schemes. Most CGL and E&O insurers now include provisions in policies that preclude coverage for these types of claims. A company that fails to insure against

these types of losses through standalone cyber coverage or a cyber endorsement may therefore be left reimbursing clients out if its own pocket.