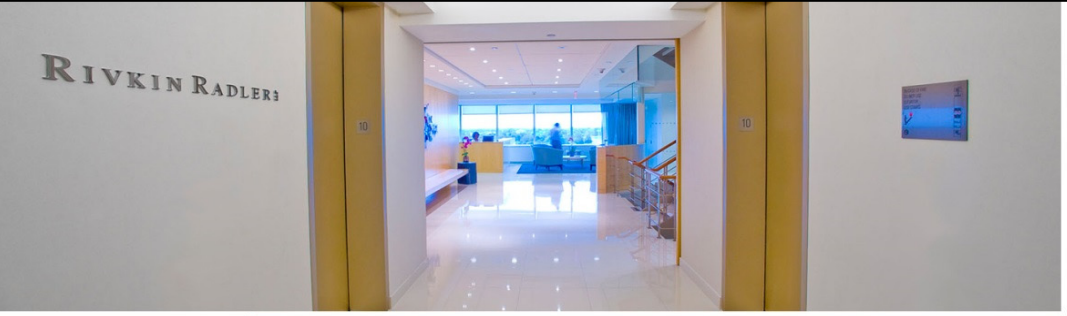

RIVKIN RADLER LLP
ATTORNEYS AT LAW

March 2021 | Insurance Update | WWW.RIVKINRADLER.COM

Arizona Supreme Court Instructs That Consent-To-Settle Provision Must be Judged from Insurer's Perspective Where Policyholder Controls Defense

On a certified question, the Arizona Supreme Court ruled that, in cases involving a liability policy without a duty to defend, the objective reasonableness of an insurer's decision to withhold consent to settle must be judged from the perspective of the insurer.

The Case

In October 2006, the stock price of the policyholder, Apollo Education Group, Inc., a higher-education services provider, dropped following revelations about an investigation into Apollo related to alleged backdating of stock options for corporate executives. A class action lawsuit was filed against Apollo in Arizona federal court.

While the appeal was pending, the plaintiffs and Apollo entered into mediation, which eventually resulted in an agreement to settle for $13,125,000. National Union refused consent to the settlement. Nonetheless, Apollo entered into the settlement agreement, paying the plaintiffs out of its own pocket. Apollo then sued National Union to recover the settlement amount, alleging both breach of contract and bad faith.

The district court granted summary judgment to National Union. Apollo appealed. The Ninth Circuit certified the following questions to the Supreme Court of Arizona: What is the standard for determining whether National Union unreasonably withheld consent to Apollo's

settlement with shareholders in breach of contract under a policy where the insurer has no duty to defend?

The Decision

The Ninth Circuit held that under a policy without a duty to defend, the objective reasonableness of the insurer's decision to withhold consent is assessed from the perspective of the insurer, not the policyholder.

The court noted that the policy's consent-to-settlement provisions spoke from the insurer's perspective because it referred multiple times to the insurer's "consent." The court concluded that it makes sense that such consent would not be viewed from the perspective of the policyholder because the policyholder has a strong and often adverse interest in settling within policy limits regardless of the merits of the claim. The court concluded that where the insurer has no control over the litigation, it is more reasonable that the insurer's perspective – which necessarily includes consideration of the merits of the claim – should prevail.

The court distinguished cases in which an insurer defends under a reservation of rights. In those cases, the court noted, the policyholder is in a precarious position because the insurer controls the litigation, yet the policyholder could still be liable for a jury verdict in excess of the policy limits and could also still be denied coverage. In such case, the court observed, there is a concern about leaving the policyholder at the risk of the insurer's mercy.

Here, by contrast, the policyholder controlled the litigation. The court stated that "[a]n equal consideration requirement [rather than from the insurer's perspective] might force an insurer to accept a settlement, controlled entirely by the insured, for the full policy limit, even if the insurer fairly valued the claim at zero or an amount below the policy limit."

The court rejected Apollo's argument that the consent-to-settlement provisions should be construed against the insurer. The court noted that, under Arizona law, where a policy is negotiated by two sophisticated parties, the rule that ambiguous policy terms are construed against the insurer does not apply.

The case is *Apollo Educ. Grp., Inc. v. Nat'l Union Fire Ins. Co.,* CV-19-0229 (Ariz. Feb. 17, 2021).

Montana Supreme Court Rules That Prior Knowledge Provisions of Claims-Made-and-Reported Policy Precluded Coverage for Legal Malpractice Claim

The Montana Supreme Court ruled that an insurer owed no duty to defend a law firm in a malpractice action where a member of the firm knew of the basis for the claim before the effective date of the claims-made-and-reported policy.

The Case

The insured law firm was accused of malpractice by a client after it failed to timely file an answer in a civil litigation, leading to a default judgment against its client.

The firm's insurer, ALPS Property & Casualty Insurance Company, sought a declaration in Montana state court that it owed no duty to defend or indemnify the firm or any of its members, for the claims filed against the firm and three of its attorneys. The claims-made-and-reported policy at issue covered claims first made against the insured and first reported to the insurer during the policy period, provided that at the effective date of the policy, no insured knew or reasonably should have known or foreseen a basis for the claim.

The trial court granted ALPS's motion for summary judgment, holding the policy did not cover the client's claim because a member of the firm knew of the basis for the claim prior to the firm's procurement of the policy. The client, the firm, and two of the firm's members, appealed.

The Decision

The Montana Supreme Court affirmed. Because a member of the firm knew of the default before the effective date of the policy, the court agreed with the trial court that the malpractice claims never fell within the policy's coverage.

Two of the supervising attorneys who were sued argued that the prior knowledge provisions did not preclude them from coverage for the malpractice claims because they had no knowledge of the underlying potential claim against the firm. But the court rejected that argument, noting that the policy did not allow a claim to be divided into parts based on the knowledge of each member. The court emphasized that the prior knowledge provisions preclude coverage for the claim, not a specific attorney. The court also observed that the supervisor attorneys' alleged failure to supervise also would have occurred prior to the policy's effective date.

The court further determined that the innocent insured doctrine did not apply to the two supervising attorneys who did not have actual knowledge of the underlying potential claim. This doctrine, the court explained, cannot be used to create coverage that otherwise would not exist.

For these reasons, the court concluded that the insurer was not required to cover the claim.

The case is *ALPS Prop. & Cas. Ins. Co. v. Keller, Reynolds, Drake, Johnson & Gillespie, P.C.* (Mont. Feb. 23, 2021).

Kentucky Supreme Court Rules That Intentional Injury Exclusion Must Be Judged by Objective Standard, But Recognizes Limited Carve-Out

The Kentucky Supreme Court ruled that application of an intentional injury exclusion must be viewed from an objective standard but found that a policyholder could assert a mental-capacity defense under limited circumstances.

The Case

A sixteen-year-old set fire to his family's home in a suicide attempt. His parents sought coverage for the fire under a homeowner's insurance policy with Auto Club Property-Casualty Company. Auto Club denied liability. The parents filed a declaratory judgment action in Kentucky state court.

The policy contained an exclusion for intentional acts that "could reasonably be expected to cause some physical damage to, or destruction of, tangible property." The trial court ruled that this exclusion didn't apply because it must be viewed from the teenager's subjective viewpoint. The trial court concluded that the teenager lacked the mental capacity to form the intent to damage the home.

The Court of Appeals reversed, and the parents appealed to the Kentucky Supreme Court.

The Decision

The Kentucky Supreme Court affirmed the Court of Appeals' reversal. The court concluded that the policy unambiguously excluded coverage for acts that, when judged objectively, could be reasonably expected by the insured to cause a loss.

However, the court left open the door for the policyholder, in the rare instance, to assert a mental-incapacity defense to defeat an intentional injury exclusion. The court noted that intentional injury exclusions are designed to prevent the insured from manipulating the risk and

receiving a financial benefit from the consequences of an intended loss. By contrast, the court observed, "an individual who lacks mental capacity to conform his conduct will not be influenced by the existence or nonexistence of coverage."

But to establish a mental-incapacity defense, the court noted that a policyholder must show at the time of the act, not merely that he did not know right from wrong, but that he did not understand the nature and quality of his actions such that he was rendered unable to understand the physical nature of their consequence. The court acknowledged that this places a "high burden on the insured."

For these reasons, the court affirmed the Court of Appeals' decision and remanded the case to the trial court to allow the insureds an opportunity to litigate the lack-of-capacity defense.

The case is *Foreman v. Auto Club Property-Casualty Ins. Co.*, 2018-SC-0618-DG (Ky. Feb. 18, 2021).

Nebraska Supreme Court Rules That Owned-Property Exclusion Bars Coverage for Negligent Misrepresentation Claim

The Nebraska Supreme Court, siding with an insurer, held that an owned property exclusion in a renters insurance policy barred coverage for a negligent misrepresentation claim.

The Case

In March 2019, Jeffrey Barkhurst filed a lawsuit against the insureds, TFG and Jeffrey Leonard, in Nebraska state court. Barkhurst alleged that when he purchased a house from TFG in August 2015, TFG failed to disclose and actively concealed several defects, including the intrusion of water, the presence of mold, substandard repairs, and structural issues. Barkhurst asserted

that TFG and Leonard were liable for breach of contract, negligent misrepresentation, and fraudulent concealment.

State Farm had issued TFG a "Rental Dwelling Policy of Insurance" (the rental policy) on January 6, 2015. TFG and Leonard submitted a claim under the policy, seeking defense and indemnity. State Farm agreed to defend TFG and Leonard under a reservation of rights.

State Farm then filed a declaratory judgment action seeking a determination that it was under no duty to defend or indemnify. The district court awarded State Farm summary judgment. TFG and Leonard appealed.

The Decision

The Nebraska Supreme Court affirmed. Even assuming that the defects in the house were caused by an accident that took place while the insured owned the property and the underlying lawsuit was one for property damage, the court noted that policy exclusions still barred coverage.

The court held that the underlying lawsuit fell within the exclusions for "property damage to property owned by any insured"; "property damage to property rented to, occupied or used by or in the care of the insured"; and "property damage or personal injury to premises [the insured] sell[s], give[s] away, or abandon[s], if the property damage, or personal injury arises out of those premises." The court noted that it was undisputed that the house was owned, in the care of, and then sold by TFG.

The court rejected TGF and Leonard's argument that the policy was ambiguous and therefore should be construed in favor of coverage. The court emphasized that an insurance policy should be read to avoid ambiguities, if possible, and the language should not be tortured to create them. Given the plain language of the exclusions, the court ruled, State Farm had no

potential liability from the underlying lawsuit under the rental policy, and thus, no duty to defend or indemnify TFG and Leonard.

The case is *State Farm Fire & Cas. Co. v. TFG Enters., LLC*, No. S-20-271 (Neb. Feb. 19, 2021).

Email Manipulation Scheme Was Not Within Computer Transfer Fraud Coverage, Fifth Circuit Holds

Affirming summary judgment in favor of an insurer, the Fifth Circuit ruled that a fraudulent email scheme that tricked the insured's employees, but not the computer itself, into transferring money into a phony account fell outside the protection of a Computer Transfer Fraud provision. That provision plainly required that the transfers be made without the insured's knowledge or consent.

The Case

The CFO of a silicon metal manufacturer received an email he thought was from one of the company's vendors. The email requested that future payments should be routed to a new bank account. Attached to the email was a letter on the vendor's letterhead and signed by the vendor's executive. The email was part of an email string that contained previous emails between the company and the vendor.

The CFO authorized two wire transfers to the new bank account totaling over $1 million dollars. The transfers were made in accordance with the company's three-step verification process. Two months later, the company discovered it had been a victim of cyber fraud.

The company submitted a claim under its commercial crime insurance policy. The policy covered Computer Transfer Fraud, Social Engineering Fraud, and Funds Transfer Fraud. The

insurer, Axis, paid the $100,000 Social Engineering Fraud limit, but denied coverage under the other provisions. Those provisions carried limits of $1,000,000.

The case concerned the Computer Transfer Fraud provision, which provided:

> The insurer will pay for loss of . . . Covered Property resulting directly from Computer Transfer Fraud that causes the transfer, payment, or delivery of Covered Property from the Premises or Transfer Account to a person, place, or account beyond the Insured Entity's control, without the Insured Entity's knowledge or consent.

Axis took the position that this coverage did not apply because the funds were transferred with the company's knowledge and the fraud was not confined to the computer system.

The insured sued Axis for declaratory judgment and breach of contract. After discovery, the parties each moved for summary judgment. The trial court ruled in favor of Axis on the basis that the loss was not caused by fraudulent computer use, but by affirmative acts of the insured's employees in initiating and authorizing the transfers. The trial court also found that the transfers were not made without the insured's knowledge or consent.

The company appealed.

The Fifth Circuit's Decision

The Fifth Circuit affirmed summary judgment in Axis's favor. But rather than focusing on whether the loss resulted *directly* from the fraud scheme, as the parties had suggested, the court instead focused on whether the Computer Transfer Fraud provision intended to cover this type of fraudulent scheme. "Computer Transfer Fraud" was defined as "the fraudulent entry of Information within a Computer System."

The insured argued that receipt of the email alone constituted "Computer Transfer Fraud" as defined by the policy. But the court determined that the mere receipt of the email was not

enough and pointed to other court decisions supporting that view. The court acknowledged that the scammers here created a fraudulent channel through which they could monitor and alter emails sent between the company and its vendor. But the court found that such email manipulation was not Computer Transfer Fraud because although the scammers gained access to the email system, they did not manipulate that system through the introduction of data or programs that could independently tell the Computer System what to do. At best, the court noted, the breach allowed the scammers to monitor the computer system and then act based on the information they learned.

And in reading the provision as a whole, the court determined that this was not the type of scheme that Axis agreed to insure. The provision only covered losses resulting from Computer Transfer Fraud that "causes the transfer . . . of Covered Property from [the Insured's account] to a[n] . . . account beyond the Insured Entity's control, without the Insured Entity's knowledge or consent." Here, the insured's employees affirmatively authorized the transfer.

The court rejected the insured's argument that it is the fraud, and not the transfer, that must be without its knowledge or consent. The court instead applied the plain language of the policy, contrasting the language of the Social Engineering Fraud coverage where an employee relies in good faith on a fraudulent instruction. By adding the "without knowledge" requirement, the policy narrowed the scope of coverage by limiting it to only those instances where the computer itself is tricked.

Having found that the insured's knowledge of the transfers precluded coverage, the court did not reach the more difficult question of whether the loss resulted directly from the fraud scheme.

The case is *Mississippi Silicon Holdings, L.L.C. v. Axis Ins. Co*., No. 20-60215 (5th Cir. Feb. 4, 2021).

Federal Court in Texas Finds That Losses from Phishing Scheme Were Not Covered by Commercial Crime Policy

A federal district court judge from the Northern District of Texas ruled that a payment-processing firm victimized by a phishing scheme was not entitled to coverage under its commercial crime policy because it did not "hold" the stolen funds despite having provided instructions to a third-party payment processor.

The Case

The insured, RealPage, provides services for real estate property managers, including collecting rents and transferring payments. It retained Stripe, a third-party software services provider, to enable payment processing and related functions.

Here's how payments were processed. A tenant would log onto one of RealPage's websites designed to look like that of one of its property manager clients. When the tenant made payment, RealPage would send application programming interface (API) calls to Stripe's server either through the Stripe Dashboard, which was accessible only to RealPage employees, or through an on-site application. Stripe would then direct its bank, Wells Fargo, to process automated clearinghouse (ACH) transfers that would pull money from the tenant's bank account and place these funds in Stripe's Wells Fargo bank account. Stripe would then instruct Wells Fargo to complete another ACH transfer to pay these fund's to client as directed by RealPage. Additionally, Stripe would conduct a separate transaction through Wells Fargo by transferring fees owed to RealPage into a different account.

Stripe was the account holder of the Wells Fargo bank account. RealPage was not entitled to draw funds from the account and did not receive interest from funds maintained in the account.

Thieves used a phishing scheme to obtain and to alter the account credentials of a RealPage employee. They then used those credentials to access the Stripe Dashboard and alter RealPage's fund distribution instructions to Stripe. The thieves diverted over $10 million that had not yet been disbursed to RealPage's clients.

After discovering the fraud, RealPage reimbursed its clients for the lost funds. It was able to recover some of the diverted transfers but was out of pocket more than $6 million. RealPage submitted a claim under its primary and excess commercial crime policies.

In short, the policies covered property that the insured owned or held for others. It also contained Computer Fraud and Funds Transfer Fraud coverages. The primary insurer agreed to cover that portion of the loss that represented RealPage's transaction fees, since RealPage owned those funds, but denied with respect to diverted funds owed to RealPage's clients on the basis that RealPage did not own or hold those funds. RealPage then sued.

The Decision

The court granted summary judgment in favor of the insurers.

The court first considered whether RealPage held the client funds. Looking to dictionary definitions, the court determined that the plain meaning of the term "hold" required possession of the property. The court rejected RealPage's broader definition that "hold' means to "control, direct, and keep under an obligation" because that definition omitted the key characteristic of "hold," which is possession.

The court next applied the plain meaning of "hold" and concluded that RealPage's authority to direct the transfer of the funds did not amount to holding the funds. The court

explained that until diverted to the thieves' account, the funds remained in an account at Wells Fargo in Stripe's name, not RealPage's. The funds were commingled with those of other Stripe users. RealPage had no rights to the funds in the account and could not withdraw them. As RealPage did not possess the funds in any way, it did not "hold" the funds.

The court similarly rejected RealPage's argument that its arrangement with its property-management clients represented a bailment. The court found that RealPage never accepted funds from its clients. Rather, it ensured that its clients received the funds from their tenants. Also, the tenants' funds were not delivered to RealPage but instead to Stripe's bank account. Stripe was not an agent of RealPage, but rather, an independent contractor. Thus, the court concluded that RealPage was not a bailee of the client funds.

Finally, the policy required that RealPage show that it suffered a loss "resulting directly from" Computer Fraud or Funds Transfer Fraud. The court noted that this language evinced an intent to limit coverage to losses sustained by RealPage, not by third parties. Because RealPage did not hold the client funds, the court concluded that RealPage's loss resulted from its decision to reimburse its clients. Thus, RealPage did not suffer a direct loss when the funds were stolen.

The case is *RealPage Inc. v. Nat'l Union Fire Ins. Co*., No. 3:19-CV-1350-B (N.D. Tex. Feb. 24, 2021).

Target's Settlements with Card Issuers Following Data Breach Were Not Loss-of-Use Damages, Minnesota Federal Court Holds

A Minnesota federal district court judge awarded an insurer summary judgment in a suit by Target seeking to recover amounts it paid to settle claims by banks for the costs to reissue credit and debit cards compromised by Target's data breach. The court found that there was an

insufficient connection between the value of the customer's inability to use the payment cards and the damages associated with that loss of use, and therefore, the claim did not qualify as "property damage" within the meaning of a commercial general liability (CGL) policy.

The Case

In December 2013, Target discovered that it sustained a data breach and that personal information about its customers, including credit and debit card information, had been stolen. Various banks that issued the compromised cards sued Target for the costs associated with reissuing payment cards to customers. Target resolved these suits through confidential settlements.

Target submitted a claim to its CGL insurer seeking indemnity for the settlements. The insurer denied coverage and Target sued.

The Decision

The court ruled that the settlements were not covered.

To demonstrate coverage, Target needed to show that the losses arose out of an "occurrence" and resulted in Target's legal obligation to pay damages because of the loss of use of tangible property that is not physically injured, a component of the "property damage" definition.

The court first assumed without deciding that the data breach constituted an "occurrence," defined as an "accident, including continuous or repeated exposure to substantially the same general harmful conditions."

The court next focused on the "loss of use" requirement. The parties' dispute centered on whether damages arising out of the payment card claims were damages based on loss of use of the payment cards.

Target argued that the settlements constituted loss-of-use damages because the compromised payment cards were no longer usable, and Target settled claims involving the cost of replacement cards.

But the court found that there must be some nexus between the value of the customer's ability to use the product or service that has been lost and the damages associated with that loss of use. By way of illustration, the court pointed to reasonable rental value as a commonly used measure of loss of use damages. Rental costs are typically viewed as loss-of-use damages because a rental car, for example, allows a driver to use a replacement car for one that has been damaged. The value of the rental represents the damages for loss of use of the driver's car.

In this case, however, there was no evidence as to what the value of the use of the payment card is to either Target's customers or to the companies that issued the cards. The court found that Target failed to establish a connection between the damages it incurred for settling the banks' claims for replacing compromised cards and the value of the use of those cards either to the payment card holders or issuers.

Because the court determined that the connection between the damages claimed and the loss of use of the payment cards was insufficiently direct, the court held that the settlement payments were not the type of loss of use damages covered by the policies. It granted the insurer's summary judgment motion.

The case is *Target Corp. v. ACE American Ins. Co.,* No. 19-cv-2916 (WMW/DTS) (D. Minn. Feb. 8, 2021).

Email Spoofing Scheme Amounted to Three Occurrence, Arizona Appellate Court Finds

A panel of the Arizona Court of Appeals found that an insured who fell victim to an email spoofing scheme was not entitled to coverage under its policy's forgery endorsement but was entitled to three full limits of the computer fraud coverage, as the insured made three separate payments after being induced by three fraudulent emails.

The Case

Thieves secretly infiltrated the email accounts of the insured's employees to intercept payments made to its vendor. Using a counterfeit domain name nearly identical to that of the vendor, the thieves created email accounts with the names of actual employees of the vendor and opened accounts at the vendor's bank. The thieves then intercepted emails transmitting insurance binders and invoices from the vendor to the insured and replaced them with fraudulent emails directing the insured to wire payments to the thieves' accounts.

Upon receiving three counterfeit emails, the insured authorized three wire transfers in excess of $350,000. Three weeks later, the vendor notified the insured that it had not received payment on the invoices. The insured notified both its bank and its vendor of the suspected fraud but was only able to recover less than a quarter of the amount transferred.

The insured submitted a claim with its business property insurer. The insured denied coverage under the Forgery and Alteration Endorsement but agreed to pay a single $10,000 per occurrence limit under the Computer Fraud coverage.

The insured sued. The insurer prevailed on summary judgment. The insured appealed.

The Appellate Court's Decision

The Arizona Court of Appeals affirmed in part and reversed in part.

It upheld the lower court's ruling that the forgery endorsement did not cover the fraudulently induced wire transfers. That endorsement applied to the forgery or alteration of negotiable instruments. The court found that the emails, including the attached insurance binders and invoices, were not endorsable instruments payable upon tender in the same manner as negotiable instruments.

The court next turned to the Computer Fraud Endorsement. That endorsement insured against "loss . . . resulting directly from the use of any computer to fraudulently cause a transfer" from inside the insured's building or its bank to a person or place "outside those premises." Recovery was limited under the endorsement to $10,000 "in any one occurrence," but the term "occurrence" was undefined in the endorsement.

The insured contended that each of the three counterfeit demands for payment that caused the insured to wire transfer funds constituted a separate occurrence. Thus, it argued it was entitled to $30,000.

The insurer, on the other hand, argued that there was only one occurrence because the cause of the loss was a single fraudulent scheme.

The appeals court sided with the insured. Applying the cause standard – whether there was one proximate, uninterrupted, and continuing cause which resulted in all injuries and damages – the court found that the thieves induced the insured through separate emails to make three wire transfers for the payment of three distinct invoices. Each fraudulent demand for payment, in the court's view, was a distinct causative act that constituted a separate occurrence.

The court distinguished cases cited by the insurer in support of its "continuing condition" argument. Unlike those cases, the Computer Fraud Endorsement here did not include the "continuous or repeated exposure to substantially the same general harmful conditions" language

often found in “occurrence” definitions, nor did it include language suggesting that multiple claims are to be treated as a single “occurrence.” The court similarly refused to treat the series of acts that led to the wire-transfers as a single incident or event.

Thus, the court held that there were three occurrences under the Computer Fraud Endorsement, and that the insured was entitled to a full $10,000 limit for each occurrence.

The case is *AIMS, Ins. Prog. Mgrs., Inc. v. Nat’l Fire Ins. Co.,* No. 1 CA-CV 20-0032 (Ariz. Ct. App. Feb. 4, 2021).