

Insurance Recovery

February 13, 2020

Fintech Company Secures Indemnity Coverage Under Professional Liability Policy for Fraudulent Funds Transfer Claim

By **Lynda A. Bennett** and **Jason D. Meyers**

What You Need To Know:

- Recent case law is trending favorably for policyholders to secure coverage for computer fraud claims under a wide array of insurance policies.
- Because several types of policies may be triggered when a computer fraud loss occurs, it is crucially important to give notice early and broadly to all insurers.
- The devil is in the details of the policy language; therefore, it is important to review and negotiate favorable policy terms at the policy placement stage and consult with experienced coverage counsel when a claim is denied.

Introduction

Recently, a Southern District of New York court, applying Connecticut law, held that AIG was required to provide indemnity coverage to a fintech company under a professional liability policy in connection with a loss sustained by a former commodities fund client. *SS&C Tech. Holdings, Inc. v. AIG Specialty Ins. Co.*, Case No. 19-cv-7859 (S.D.N.Y. Jan. 29, 2020). This decision is significant because insurers frequently deny coverage for social engineering and funds transfer fraud claims. However, several recent court decisions across the country have been favorable to policyholders who have pursued coverage under a wide array of policies, including dedicated cyber, crime, and, here, professional liability. In this case, the court rejected the insurer's attempt to rely on an exclusion to avoid its coverage obligation because the insurer could not carry its burden to demonstrate that the exclusion applied and because the exclusion contained ambiguous language, which must be construed in favor of coverage.

Factual Background

SS&C is a fintech company that provides business processing management services to its clients. In early 2016, unidentified fraudsters used spoofed email domains to send SS&C fraudulent fund transfer requests that appeared to originate from an SS&C fund client. In response, over the course of a few weeks, SS&C processed approximately \$5.9 million of fraudulent wire transfers from its client's account to bank accounts in Hong Kong.

Defense and Indemnity Coverage

The fund client sued SS&C for gross negligence in handling the client's funds. AIG was SS&C's professional liability insurer and agreed to defend SS&C but denied coverage for any settlement based on an exclusion in the policy "for the monetary value of any funds lost due to the Insured'[s] exercise of ... authority or discretionary control ..." AIG focused on this particular exclusion because the policy's cyber extortion exclusion was narrow and inapplicable.

SS&C then settled with its former client and, in turn, sued AIG.

In the coverage lawsuit, the trial court concluded that SS&C had no **independent** authority to process transactions apart from its former client's authority based on the language of the services agreement with the client, which stated that the management and control of the fund were vested exclusively in the fund. AIG argued that SS&C had authority and discretion over the client's funds because five SS&C employees were identified as "Authorized Signers" on the client's account and could sign checks and withdraw funds from the client's account. The court rejected AIG's argument, noting that AIG was "conflating SS&C's administrative ability to operate [the client's] account, which indisputably existed, with SS&C's authority and discretionary control over that account." While SS&C employees had the ability to sign checks and facilitate transfers, the court found, they could take those actions only after receiving instructions from the fund.

The court also rejected AIG's attempt to sidestep its indemnity coverage obligation by arguing that the exclusion applied to funds that were "lost"—a term that was not defined in the policy. The court acknowledged that both SS&C and AIG offered plausible interpretations of what constituted "lost" funds (i.e., "missing" (SS&C) and "stolen" (AIG)). As such, the court concluded that the term was ambiguous and therefore must

be interpreted in favor of the insured. Thus, the court found that the exclusion did not apply and ordered AIG to cover SS&C's settlement in the underlying lawsuit.

Key Takeaways

Courts vary with respect to a policyholder's ability to recover loss for social engineering and funds transfer fraud claims. Based on relevant state law and the terms of the policy, courts have come to opposite conclusions on whether a policyholder may obtain coverage. Though cyber insurance policies typically provide the best option to secure coverage for computer fraud claims, policyholders should not overlook the coverage that may be available from other traditional policies included within their insurance program. When presented with a computer fraud claim, policyholders are well served to immediately give notice to all insurers who may provide coverage for computer- and data-related claims. In addition, policyholders should not just take no for an answer when an insurer has denied coverage. It is not uncommon for insurers to revisit their coverage position after knowledgeable coverage counsel has been engaged to dispute a claim denial. The onus is on insurers to prove that a policy exclusion clearly and unambiguously applies, and recent case law is trending favorably for policyholders to recover insurance proceeds for computer fraud claims.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

LYNDA A. BENNETT

Partner

T: 973.597.6338

lbennett@lowenstein.com

JASON D. MEYERS

Associate

T: 973.597.2310

jmeyers@lowenstein.com

NEW YORK

PALO ALTO

NEW JERSEY

UTAH

WASHINGTON, D.C.

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.