

TUESDAY, DECEMBER 3, 2019

## PERSPECTIVE

## Insureds seek coverage for breaches under traditional policies

By Peter S. Selvin

There have been a number of high-profile insurance coverage cases arising from losses due to cyber fraud — especially data breaches, “spoofing” and payment instruction fraud. While cyber insurance is specifically designed to address these kind of losses, insureds covered under traditional insurance products such as commercial general liability, errors and omission, and crime policies have continued to seek coverage under those policies for cyber-related losses.

For example, in a case filed on Nov. 15, Target seeks recovery for its cyber fraud-related losses from its general liability carrier Ace American Insurance Company. The case arose from Target’s discovery in 2013 that a hacker had installed malware on its computer network which had allowed the hacker to gain access to customer payment card and other personal data. According to Target’s complaint, the data breach enabled the hacker “to steal payment card data and personal contact information for millions of Target customers, exposing those customers to the risk of fraudulent transactions on their payment cards.”

As a result of these events, the banks that had issued the payment cards to Target’s customers “were required to dedicate substantial resources to cancelling and reissuing physical payment cards.” The issuing banks subsequently sued Target for their losses, which included “losses directly caused by the replacement of the physical cards.”

After settling with the issuing banks, Target brought an action against Ace. Its general liability policy with Ace obligated Ace to pay Target for “property damage,” which was defined to include “loss of use of tangible property that is not physically injured.” According to its complaint, coverage under the general liability policy was satisfied because the issuing banks “sought damages [from

Target], for, among other things, loss of use of tangible property (i.e., physical plastic payment cards) that, while not physically injured, could not be used without risk to the customer and the bank.”

The Target suit is noteworthy because it represents another example of insureds seeking coverage for cyber-related losses from traditional insurance policies. As one commentator has noted, this trend of “silent cyber”

**While cyber insurance is specifically designed to address these kind of losses, insureds covered under traditional insurance products such as commercial general liability, errors and omission, and crime policies have continued to seek coverage under those policies for cyberrelated losses.**

relates to “the possibility that insurance coverage for cyber-related losses may be found in other insurance policies, policies that the insurers would argue were not built with the possibility of coverage for cybersecurity related losses in mind.” Kevin La Croix, “Seeking Insurance for Cybersecurity-related Losses,” *The D & O Diary* (Nov. 24, 2019).

Another recent case also exemplifies this trend. In *SS&C Technology Holdings, Inc. v. AIG Specialty Insurance Company*, 19-cv-7859 (S.D.N.Y. 2019), SS&C wired funds out of a client’s account in reliance on email instructions purportedly from the client. Instead, the email, although appearing to be genuine, was generated by a fraudster and the funds ended up in the fraudster’s account.

This kind of scenario is called “spoofing” or “social engineering fraud,” and several recent cases have addressed whether losses arising from these circumstances are recoverable under computer fraud coverage. *See, e.g., Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. Appx. 252, 258 (5th Cir. 2016) (no coverage); *Taylor &*

*Lieberman v. Federal Insurance Company*, 2017 WL 929211 (9th Cir. 2017) (same); *Medidata Solutions, Inc. v. Federal Insurance Company*, 268 F.Supp.3d 471 (S.D.N.Y. 2017), *aff’d*, 729 Fed. Appx. 117 (2nd Cir. 2018) (coverage found).

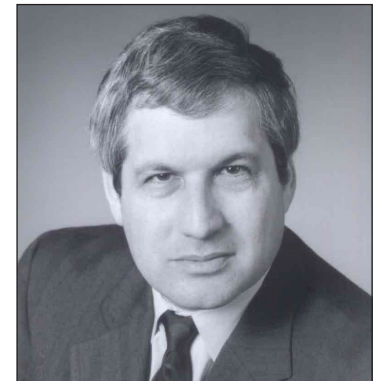
Following the “spoofing incident,” SS&C settled with its client and then sought recovery against its errors and omissions carrier AIG Specialty Insurance Company. As in the Target

arguing that this exclusion applied not only to any dishonest, fraudulent, criminal or malicious act committed by SS&C but also to such acts committed by third-party fraudsters, such as those involved in the “spoofing” incident at bar.

In a decision issued on Nov. 5, U.S. District Judge Jed Rakoff denied AIG’s motion to dismiss. The noted that “even though reading the first clause [of the exclusion] might support AIG’s interpretation, this interpretation falters when the sentence is read in its entirety. For coupling the first clause with the ‘provided, however’ clause of the same sentence clearly indicates that [the exclusion] applies only to dishonest, fraudulent, criminal...acts by SS&C not to these such acts committed by third-party fraudsters.”

The decision in SS&C has implications beyond the errors and omissions context as the exclusion at issue in that case is a standard feature of directors and officers policies. The decision in SS&C also highlights the same “silent cyber” trend discussed above. In this regard, other courts have found coverage for cyber-related losses under errors and omissions policies. *See, e.g., Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010); *Stark & Knoll Co. L.P.A. v. ProAssurance Cas. Co.*, 2013 U.S. Dist. LEXIS 50326 (N.D. Ohio Apr. 8, 2013). ■

**Peter S. Selvin is now a Partner with Ervin Cohen & Jessup LLP**



suit, SS&C made resort to a traditional insurance product — in this case an errors and omissions policy — for recovery of losses arising from cyber fraud. AIG denied SS&C’s claim and SS&C brought suit.

Under the errors and omission policy, AIG was obligated to pay on SS&C’s behalf losses resulting from a claim alleging a “wrongful act,” which was defined to include “any negligent act, error or omissions, misstatement or misleading statement in [SS&C’s] performance of Professional Services for others.”

The policy also had an exclusion which barred coverage for losses in connection with claims “alleging, arising out of, based upon or attributable to a dishonest, fraudulent, criminal or malicious act, error or omission, or any intentional or knowing violation of the law; provided, however, [AIG] will defend Suits that allege any of the foregoing conduct, and that are not otherwise excluded, until there is a final judgment or final adjudication against an insured in a Suit.”

Relying on this exclusion, AIG moved to dismiss SS&C’s suit,