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 kinds 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 (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” policies has continued to seek coverage under those policies for cyberrelated losses.

While cyber insurance is specifically designed to address these kinds 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.

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 case arose from the first clause of the exclusion and the court ruled that “even though reading the first clause of the exclusion might support AIG’s interpretation, this interpretation fails 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 those 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 Cos. 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