Privacy and Data Security Alert: Are Credit Card Company Assessments and Penalties Covered by Your Cybersecurity Insurance Policy?

March 22, 2016

Cyber criminals frequently target credit card information that they can quickly sell on the black market. Because of the widespread nature of these types of attacks, more companies are now buying cybersecurity insurance. Such policies may provide coverage for costs associated with notifying customers of a breach, implementation of credit monitoring, dealing with regulators, and resolving claims by customers.

But there is another cost associated with the fraudulent use of stolen credit card information: namely, the credit card company's chargeback of the fraudulent purchases and other costs to the merchant, as well as fines and penalties for failure to comply with the Payment Card Industry (PCI) Data Security Standards (DSS). Whether and to what extent such losses are covered by a cybersecurity policy is front and center in a recent case involving a cyberattack at a hotel in New Orleans. *New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London*, U.S. Dist. Ct. File No. 2:16-CV-00061 (E.D. Louisiana).

According to the complaint, in 2013 Hotel Monteleone suffered a cyberattack involving credit and debit cards resulting in credit card chargeback liabilities being assessed against the hotel. At the time, the hotel had no insurance to cover these losses. As a result, in 2014, the hotel purchased an Ascent CyberPro policy. The Security and Privacy Liability insuring section of the policy has a limit of $3 million. The policy also has a "Payment Card Industry Fines and Penalties" endorsement with a sublimit of $200,000. That means that the most the insurer will pay for PCI fines and penalties is $200,000. The following year (2015), the hotel purchased another Ascent CyberPro policy. This policy also contained a "Payment Card Industry Fines and Penalties" endorsement, but the language was broadened to include "reimbursements, fraud recoveries or assessments" that the hotel would owe under a merchant services agreement with a credit card association.

While the 2014 policy was in effect, the hotel suffered another cyberattack involving credit and debit cards. As a result, MasterCard assessed the hotel for four types of losses:

1. Account Data Compromise (ADC) Fraud Recovery (losses from fraudulent charges);
2. ADC Operational Reimbursement (losses for replacing payment cards);
3. Case Management Fees (investigation and other costs incurred by MasterCard);

4. And fines and penalties for alleged violations of PCI-DSS.

In total these losses are alleged to exceed $200,000.

The hotel turned to Ascent to cover the losses. Ascent took the position that the PCI Fines and Penalties endorsement applied not only to the PCI-DSS fines and penalties, but the fraud recovery, operational reimbursement and case management fees arising out of the breach. Accordingly, only $200,000 was available to pay all of the losses. On the other hand, the hotel took the position that the fraud recovery, operational reimbursement, and case management fee losses were covered by the Security and Privacy Liability section of the policy and thus subject to the full $3 million limit, not the $200,000 sublimit. In that regard, the hotel cites the 2015 Fines and Penalties endorsement, which expressly includes fraud recovery, operational reimbursement and case management fees, as proof that the 2014 endorsement did not include such losses. The litigation has been stayed pending conclusion of mediation.

Cyber policies are very complex and filled with specialized terms and conditions. Many of these provisions have not been judicially tested. As the *Monteleone* complaint illustrates, when a loss occurs, the insurer is likely to parse the language in its favor. It is therefore important for policyholders to carefully review the policy and ask questions during the underwriting process (when the insurer is anxious to close the deal), rather than getting embroiled with the claims department after a loss occurs. It is particularly important to understand the endorsements as they can dramatically affect the scope of coverage.