BARNES & THORNBURG LLP

What Insurance Should Cover Target's Visa Settlement?

August 20, 2015 | | Cyber Insurance, Data Breach, Policyholder Protection

Scott N. Godes
Partner
Data Security and Privacy Co-Chair, Insurance Recovery and Counseling Group Co-Chair

insuranceblogpic**Two years later, and the Target data breach continues to make headlines.** Does anyone need to be reminded that Target suffered a data breach in 2013? Seeing that the breach continues to be litigated and settlements continue to be announced with payment card brands, it is difficult to forget the incident. Most recently, Target announced that it had reached a settlement with Visa.[1] According to reports, Target could "pay as much as $67 million to banks that issue Visa cards."[2] Target's earlier $19 million settlement with MasterCard[3] ended up being scuttled; Target and MasterCard reportedly are working on another resolution.[4]

What is Target settling? Target's settlement with Visa likely is to resolve the alleged damages resulting from Target's payment card breach. The payment card brands allegedly act on behalf of the issuing banks, seeking recovery of damages for the issuing banks' alleged losses resulting from a retailer's data breach.[5] The payment card brands seek damages from the retailers, asserting that the retailers are responsible for the fraudulent charges that were incurred and the amounts spent to replace payment cards. **What insurance policies should cover these settlements?** We previously discussed whether Target's cyberinsurance would cover the earlier proposed $19 million settlement with MasterCard.[6] And we concluded with a bold, "*Probably*." We reached that conclusion after reviewing writings by insurance underwriters, who would have policyholders boxed in to a certain kind of coverage in a cyberinsurance policy to cover the losses, as well as Target's filing explaining that it has $50 million in sublimited coverage in its network security insurance policies (*i.e.*, cyberinsurance) for this exact type of loss.[7] What about other coverage? Would commercial general liability (CGL) insurance policies cover? We previously have asserted that CGL policies should provide coverage for retailers that have suffered a data breach. The previous post discussed putative class action claims against retailers post-data breach. CGL policies, in our view, also should provide coverage for demands by the payment card brands after a credit card data breach. As discussed previously, CGL policies should be read to provide coverage for damages because of both property damage and personal and advertising injury for losses resulting from a data breach. We believe that the financial liabilities to the payment card brands, payment card processors, or acquiring banks also could be viewed as covered under a CGL policy. A

RELATED PRACTICE AREAS

Data Security and Privacy
Insurance Recovery and Counseling

RELATED TOPICS

cyber insurance
data breach
retailers
Settlement

typical CGL insurance policy states that the insurance company will pay those sums that the insured becomes legally obligated to pay as damages because of property damage or personal and advertising injury. Are the assessments from payment card brands "damages"? For purposes of an insurance analysis, we believe that the amounts paid to the card brands, processor, or acquiring bank could be viewed as resolving financial liabilities, and the resolution of those liabilities could be viewed as damages. It should be seen as a basic insurance coverage principle that a settlement of a financial liability meets the definition of "damages." Money taken by the payment card processor or acquiring bank should be seen as a resolution of financial liabilities. And, in the words of MasterCard and Visa documents, the amounts paid to resolve the financial liabilities may be viewed as "settlements." In the MasterCard *Account Data Compromise User Guide*, (June 26, 2014), it states that the final step in a credit card data breach privacy incident is the:

> "financial settlement of losses encountered as a result of an ADC [Account Data Compromise] Event, including operational reimbursement, fraud recovery, and ADC Event case management."[8]

A version of Visa's Global Compromised Account Recovery Guide (GCAR) that may be found on the web defines Visa's imposition of financial liability as an acquiring bank "Settlement."[9] In sum, if the insured were legally obligated to pay "damages" (settlement of financial liability) because of property damage (loss of use of credit cards) or personal and advertising injury (publication of private information), the requirements a CGL policy's insuring agreement should be viewed as being satisfied. **Takeaways** The Target payment card data breach continues to provide food for thought when it comes to insurance coverage and risk transfer. New information that develops about Target's liabilities, and resolution of them, provides a good time to evaluate how insurance would cover the losses. Policyholders should consider using announcements like this as an opportunity to evaluate their insurance program and consider how the policies would apply. [1]Shannon Pettypiece & Elizabeth Dexheimer, *Target Reaches $67 Million Agreement with Visa Over Breach*, Bloomberg Business (Aug. 18, 2015), available at http://www.bloomberg.com/news/articles/2015-08-18/target-says-it-has-reached-settlement-with-visa-over-data-breach. [2] *Id.* [3] Scott Godes, *Will Cyberinsurance Cover Target's $19 Million Settlement With MasterCard?*, BT Policyholder Protection Blog (April 20, 2015), available at https://www.btpolicyholderprotection.com/will-insurance-cover-targets-19-million-mastercard-settlement/. [4] Robin Sidel, *Target to Settle Claims Over Data Breach*, Wall Street Journal (Aug. 18, 2015), available at http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013. [5] MasterCard's Security Rules and Procedures could be read to suggest that MasterCard is acting as an agent for issuing banks and demands against retailers are made on behalf of the issuing banks in whole or in part. MasterCard, *Security Rules and Procedures – Merchant Edition*, § 10.2.5.3 (Feb. 5, 2015) available at http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf. Visa's Global Compromised Account Recovery (GCAR) Guide also could be read to suggest that Visa is acting as an agent pursuing the damages that issuing banks allegedly suffered as a result of fraudulent charges and replaced cards. Visa, Inc., *Visa Core Rules and Visa Product and Service Rules*, at 521 (Apr. 15, 2015), available at http://usa.visa.com/download/about_visa

/15-April-2015-Visa-Rules-Public.pdf. [6] Scott Godes, *Will Cyberinsurance Cover Target's $19 Million Settlement With MasterCard?*, BT Policyholder Protection Blog (April 20, 2015), available at https://www.btpolicyholderprotection.com/will-insurance-cover-targets-19-million-mastercard-settlement/. [7] *Id.* [8] MasterCard, *Account Data Compromise User Guide*, at 7-1 (June 26, 2014), available at http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf. [9] Visa, Inc., *Visa Global Compromised Account Recovery Guide (GCAR)*, at 29 (Jan. 2015), available at https://www.icba.org/files/Bancard/PDFs/GlobalCompromiseAccountRecoveryGuide01142015.pdf.