BARNES & THORNBURG LLP

Will Cyberinsurance Cover Target's $19 Million MasterCard Settlement?

April 20, 2015 | Data Breach,Insurance,Policyholder Protection

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

Another credit card in the mail?

If you're reading this post, you've probably received a new credit or debit card in the mail, attached by rubber cement to a cover letter explaining that your card number could have been compromised - so you ended up with replacement cards. You might even have received new cards more than once over the past five years. Perhaps you even received a new card with an explanation that after the data breach at Target Corporation, your "issuing bank" – the bank that issued you the credit or debit card – decided to send you a new card. And maybe you signed your card, called to activate it, replaced your old card, and didn't give a second thought to it. After all, consumers generally are not financially responsible for fraudulent charges and likely did not pay to get the shiny new piece of plastic in the mail.

What are card brand liabilities?

The payment card brands, however, view such incidents differently than do individual consumers. The payment card brands frequently pursue retailers, either directly or by means of a payment processor. They allegedly do so on behalf of the issuing banks and the losses that the issuing banks allegedly suffered as a result of the data breach.[1] The brands allege that the retailers are responsible for the fraudulent charges that were incurred and the amounts spent to replace payment cards. As Target explained in its 2014 Form 10-K:

> "In the event of a data breach where payment card data is or may have been stolen, the payment card networks' contracts purport to give them the ability to make claims for reimbursement of incremental counterfeit fraud losses and non-ordinary course operating expenses (such as card reissuance costs) that the payment card networks believe they or their issuing banks have incurred as a result of the event." [2]

Those amounts can run into the millions of dollars (Card Brand Liabilities).

RELATED PRACTICE AREAS

- Commercial General Liability
- Copyright, Trademark, and Media Liability
- Credit and Mortgage Insurance
- Data Security and Privacy
- Directors and Officers Liability
- Employment Practices Liability
- Fidelity Bonds and Commercial Crime Policies
- First-Party Property
- Insurance Recovery and Counseling
- Ocean Marine and Cargo Coverage
- Professional Liability
- Representations and Warranties
- Workers' Compensation and Employers' Liability

RELATED TOPICS

- Data Breach

Card Brand Liabilities also may include amounts for alleged failures to maintain certain levels of computer security required by contract (so-called PCI-DSS compliance).[1] The amounts owed for alleged fraudulent charges and replacement of compromised credit cards often dwarfs the amounts of fines for alleged PCI non-compliance.[2] Some incidents that involved more than 1 million allegedly exposed card numbers have resulted in Card Brand Liabilities in the millions of dollars.[3]

Target's card brand liabilities…and pending settlement of them with MasterCard

Target disclosed that three out of the four payment card brands made written demands for Card Brand Liabilities, and that it expected the fourth brand to do so as well.[4] The total amount of Target's potential Card Brand Liabilities is unclear, but Target did disclose that it had incurred $252 million of data breach-related expenses, an amount that accounts for Card Brand Liabilities.[5] On April 15, 2015, Target announced that it had reached a settlement of its Card Brand Liabilities with MasterCard for up to $19 million.[6] Interestingly, Target explained that the settlement is contingent upon the issuing banks, which allegedly reimbursed the fraudulent charges and issued the new cards, agreeing to accept payment via the MasterCard settlement and the issuing banks dropping claims against Target.[7] This requirement is fascinating, as issuing banks have filed a putative class action against Target directly, alleging that they suffered losses as a result of Target's data breach.[8] It may be that the MasterCard settlement resolves at least part of the claims at issue in the issuing bank litigation.

Will Target's cyberinsurance cover its card brand liability settlement?

Now for the question you've been waiting for: will Target's insurance policies cover its $19 million settlement with MasterCard? *Probably*. Without commenting on the correctness of the position, consider that one underwriter has written that Card Brand Liabilities are contract-based indemnities and may be excluded from cyberinsurance coverage, with emphasis added:[9]

Many policy forms in the marketplace directly exclude contractual indemnities and liability, including that which stems from merchant service agreements. Some policy forms initially grant coverage for breach of contract claims, but then add exclusions concerning key components of this coverage. In addition, some policy forms exclude breach of contract claims with some very narrow carvebacks to the exclusionary wording that may not help the insured much in the event of a payment card breach. Although most privacy/security insurance policies grant the insured coverage for situations in which they need to incur the first-party costs to notify individuals and extend insureds credit monitoring services, *not all will directly respond to the breach of, or the indemnities contained in, a merchant services agreement*.

Without commenting on the merits of it, consider an opposing view that Card Brand Liabilities could be treated as common law claims for purposes of insurance coverage, not liabilities created by contract, and the payment card brands are demanding amounts as agents for the issuing banks. Target may not have to address whether its Card Brand Liabilities were created by merchant services agreement contracts or are common law liabilities, because Target reportedly has $50 million in coverage for this exact type of

loss:

> "To limit our exposure to losses relating to data breach and other claims, we maintain $100 million of network-security insurance coverage, above a $10 million deductible and with a $50 million sublimit for settlements with the payment card networks."[10]

How would your insurance cover card brand liabilities? Even if you have cyberinsurance, does the policy address card brand liabilities? Does your insurance carrier's claim handler view the losses as liabilities under a merchant services agreement contract? Or as common law liabilities? If it's the former, are there exclusions for liabilities allegedly assumed in a merchant services agreement contract? Or sublimits on the total policy limit (making just a fraction of coverage available)? Consider using the Target announcement as a perfect opportunity to review your insurance – including your cyberinsurance – policies closely to figure out whether you would have full coverage for these losses. The last thing that you want to face is the prospect of your insurer denying coverage for millions of dollars in losses after you were told that buying cyberinsurance would be a panacea for all things cyberrisk.

[1] *See, e.g.*, *First Bank of Del., Inc. v. Fid. & Deposit Co. of Md.*, 2013 WL 5858794, at *2 (Del. Super. Oct. 30, 2013), *rearg. denied*, 2013 WL 6407603 (Del. Super. Dec. 4, 2013). [2] *Genesco, Inc. v. Visa U.S.A., Inc.*, 296 F.R.D. 559, 564 (M.D. Tenn. 2014) (over $13 million in liabilities overall, but only $10,000 in "fines for failing to ensure Genesco's PCI DSS compliance"), *opinion amended and superceded on other grounds*, 2014 WL 935329 (M.D. Tenn. Mar. 10, 2014). [3] *See, e.g.*, *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, 691 F.3d 821, 824-25 (6th Cir. 2012) (retailer suffered more than $4 million in Card Brand Liabilities after credit card-based data incident); *First Bank of Del.*, 2013 WL 5858794, at *2 (bank and debit card processor paid $1.4 million in compensatory damages due to Card Brand Liabilities after data incident of retailer with whom company did business); *Genesco, Inc. v. Visa U.S.A., Inc.*, 296 F.R.D. 559, 564 (M.D. Tenn. Jan. 14, 2014) ($13.3 million in Card Brand Liabilities after a credit card-based data incident). [4] Target, *Form 10-K*, Target Corporation SEC Filings (Mar. 14, 2014) [5] Target, *Form 10-K*, Target Corporation SEC Filings (Mar. 14, 2014). [6] Target, *Target Announces Settlement Agreement with MasterCard; Estimated Costs Already Reflected in Previously Reported Results* (Apr. 15, 2015). [7] *Id.* [8] *See* *In re Target Corp. Customer Data Security Breach Litigation (Financial Institution Cases)*, MDL No. 14-2522 (PAM/JJK), slip op. (D. Minn. Dec. 2, 2014). [9] Matt Donovan, *Banking on Credit: Merchants bear the brunt of data breach risks in the hospitality industry*, PropertyCasualty 360º (Dec. 1, 2013) (emphasis added). [10] Target, , *Form 10-Q*, Target Corporation SEC Filings (Nov. 26, 2014). [1] 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). [2]Target, *Form 10-K*, Target Corporation SEC Filings (Mar. 14, 2014).