BARNES & THORNBURG LLP

# If Your System Was Attacked By "Backoff" Malware, Would Your Insurance Cover A Data Breach Involving Credit Card Numbers?

August 28, 2014 | Cyber Insurance, Data Breach, Policyholder Protection

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

Silver laptopThe US Federal Government recently issued an alert regarding Backoff Point-of-Sale Malware. The advisory, which was released by the DHS (Department of Homeland Security) and US-CERT (United Stated Computer Emergency Readiness Team), states the following:

> This advisory was prepared in collaboration with the National Cybersecurity and Communications Integration Center (NCCIC), United States Secret Service (USSS), Financial Sector Information Sharing and Analysis Center (FS-ISAC), and Trustwave Spiderlabs, a trusted partner under contract with the USSS. ***The purpose of this release is to provide relevant and actionable technical indicators for network defense against the PoS malware dubbed "Backoff" which has been discovered exploiting businesses' administrator accounts remotely and exfiltrating consumer payment data.***

US-CERT, *Alert (TA14-212A), Backoff Point-of-Sale Malware*, Department of Homeland Security (Aug. 22, 2014 revision) (emphasis added). DHS estimates that over 1,000 US businesses have been affected by the Backoff malware:

> Over the past year, the Secret Service has responded to network intrusions at numerous businesses throughout the United States that have been impacted by the "Backoff" malware. Seven PoS system providers/vendors have confirmed that they have had multiple clients affected. Reporting continues on additional compromised locations, involving private sector entities of all sizes, and the Secret Service currently estimates that over 1,000 U.S. businesses are affected.

*Id.* What does that mean for affected businesses? DHS reports that the Backoff malware can compromise point-of-sale systems, with these results:

> After ***gaining access to what was often administrator or privileged access accounts***, the suspects were then able to deploy the point-of-sale (PoS) malware and subsequently exfiltrate consumer payment data via an encrypted POST request.

* * *

> The impact of a compromised PoS system can affect both the businesses and consumer by ***exposing customer data such as names, mailing addresses, credit/debit card numbers, phone numbers, and e-mail addresses to criminal elements***. These breaches can impact a business' brand and reputation, while ***consumers' information can be used to make fraudulent purchases or risk compromise of bank accounts***. It is critical to safeguard your corporate networks and web servers to prevent any unnecessary exposure to compromise or to mitigate any damage that could be occurring now.

*Id.* (emphasis added). What rarely is reported for these types of incidents are liabilities that retailers potentially face to the payment card brands after cyberattacks of this nature. Those amounts can run into the millions of dollars ("Card Brand Liabilities"). Often the most significant portion of Card Brand Liabilities are for losses due to fraudulent charges and replacing cards that had their numbers exposed. 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. *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).] 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. *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).] Some incidents that involved more than 1 million allegedly exposed card numbers have resulted in Card Brand Liabilities in the millions of dollars.[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.*, --- F.R.D ---, 2014 WL 199858, at *1 (M.D. Tenn. Jan. 14, 2014) ($13.3 million in Card Brand Liabilities after a credit card-based data incident).] When viewing Card Brand Liabilities as a big picture question, the total amounts can be viewed as a multiplier based on the number of cards exposed, with some retailers suffering liabilities of approximately $2-3 per allegedly exposed card number.[4. *Id.*] Target Corporation has disclosed that "[i]n the fourth quarter of 2013," it had accrued "$61 million of pretax Data Breach-related expenses," including "an accrual related to the expected payment of payment card networks' claims by reason of the Data Breach."[5. Target, *Form 10-K*, Target Corporation SEC Filings (Mar. 14, 2014), available at http://investors.target.com/phoenix.zhtml?c=65828&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTk0NjY2MjYmRFNFUT0wJlNFUT0wJlNRREVTQz1TRUNUSU9OX0VOVElSRSZzdWJzaWQ9NTc%3d. ] Would your insurance policy cover those amounts? Insureds should read their "cyberinsurance" policies very closely. Without commenting on the correctness of the position, consider that one underwriter has written the following, with emphasis added:[6. Matt Donovan, *Banking on Credit: Merchants bear the brunt of data breach risks in the hospitality industry*, PropertyCasualty 360º (Dec. 1, 2013), available at http://www.propertycasualty360.com/2013/12/01/banking-on-credit?t=commercial (emphasis added). ]

> 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

## RELATED PRACTICE AREAS

Data Security and Privacy
Insurance Recovery and Counseling

## RELATED TOPICS

Credit Cards
cyber insurance
Department of Homeland Security
NCCIC

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***.

Are you sure as to how your insurance would apply to card numbers stolen, published, and/or exfiltrated by the Backoff virus? Perhaps now is the time to review your insurance policies to better understand the potential for coverage, in light of this widespread risk. Amounts owed to the card brands from incidents like this can run into the millions of dollars, and obtaining insurance coverage for these losses may be crucial.