LESSONS LEARNED FROM THE TARGET DATA LOSS ABOUT SUBROGATION CLAIMS AGAINST INFORMATION TECHNOLOGY ("IT") COMPANIES

BY G. ANDREW ("ANDY") ROWLETT

Howell & Fisher, PLLC

This article was originally published in the *Subrogator*, a publication of the National Association of Subrogation Professionals, Winter 2015, Pages 60-63.

The 2013 hack of Target's customer data was the largest known such loss to date for a U.S. retailer.[1] One estimate of the loss exceeds $18 billion.[2] It involved 110 million customers.[3] Analysis of a recent lawsuit filed by two banks against Target and Trustwave, Target's third party IT (information technology) services provider, may be instructive for subrogation claims alleging inadequate IT services. This article examines the complaint filed in that case so that subrogators may consider its possible applicability to claims they may make against thirty party IT services providers.

During November and December 2013, hackers gained access to Target's network and point-of-sale ("POS") system and took private information of customers.[4] Stolen information went to a computer in Russia multiple times.[5] Users of the information were able to make fake credit cards and fraudulent purchases and to take money from victims' bank accounts.[6] Banks such as the plaintiffs have had to reissue stolen cards and cover fraudulent charges.[7] Plaintiffs describe the damage as "monumental."[8] The lawsuit by Trustmark National Bank and Green Bank was filed on March 24, 2014, in the U.S. District Court in Chicago, No. 1:14-cv-02069.[9]

Because Trustwave is the third party IT services company whose potential liability is the focus of this article, only the claims that include Trustwave and their possible applicability to claims by a subrogating carrier against an IT vendor are discussed below.

---

[1] Complaint p. 1; http://www.bloomberg.com/infographics/2014-05-14/target-data-breach.html.
[2] Id. at ¶ 93; http://www.csoonline.com/article/2138440/network-security/banks-dismiss-claims-against-trustwave-and-target.html.
[3] Id. at ¶ 3.
[4] Id. at ¶ 33.
[5] Id. at ¶ 1; 59.
[6] Id. at ¶ 60.
[7] Id. at ¶ 91.
[8] Sect. i on p. 28 of the complaint.
[9] Strangely, the action was dismissed by the plaintiffs voluntarily without prejudice at the end of March 2014. As of the time this article was submitted for publication, there was no explanation from the plaintiffs for the dismissals nor had the action been re-filed.

(1) Plaintiffs allege that the IT company was responsible was monitoring for system intrusions and reporting to Target re said intrusions.[10] Even though the company was supposed to identify intrusions quickly, the data breaches continued for three weeks. Either the IT company failed to learn of system intrusions or it learned of them and failed to report them to Target. Plaintiffs cited both industry standards and the IT company's promises in support of plaintiffs' claims on this point. [11] (Trustwave denied that Target outsourced its data security or IT obligations to Trustwave, that Trustwave monitored Target's network, and that Trustwave processed cardholder data for Target.[12])

(2) The complaint quotes the IT company's statements about its deep expertise and experience in the area of information security.[13] Consider what a potentially responsible IT vendor represented about its capabilities and work history.

(3) Plaintiffs asserted that Target's adoption of certain industry standards and its statements to the public about meeting those standards imposed a duty not only on Target but also on Trustwave. Consider whether your insured's actions caused certain standards to apply to a potentially responsible IT company hired to assist it.

(4) Industry standards are often central to large property subrogation claims. For example, NFPA 921 is key in fire losses. The complaint in the Trustwave case discussed in detail the main industry standard for preventing data breaches such as the one at Target, PCI DDS.[14] These standards were issued by the PCI Security Standards Council.[15] Just as a subrogating carrier would look to the NFPA for applicable standards in a fire case, it should identify controlling industry standards for an IT case.

(5) White papers by experts may also help establish industry standards. In the Trustwave case, an expert's white paper from 2007 explained exactly how to prevent a data breach such as the one from which this action arose.[16] The complaint describes proof that Target at least received the white paper in question.[17]

(6) Statutes and regulations may support a claim for negligence per se and/or establish an industry standard. Plaintiffs in this case cited Minnesota's Plastic Card Security Act and federal Red Flag Rules.[18] They also cited federal regulations promulgated under the Fair and Accurate Credit Transaction Act (FACTA) and industry Card Operating Regulations.[19]

(7) An IT company's violation of standards and regulations may support a negligence per se claim. This was alleged by plaintiffs.[20] As in all negligence per se claims, the injured parties must be among those intended to be protected by the cited standards.[21]

---

[10] Complaint at ¶ 85.
[11] Id. at ¶ 86.
[12] See http://bhconsulting.ie/securitywatch/?p=2084.
[13] Complaint at ¶ 81-82.
[14] Id. at ¶ 75, 80.
[15] See https://www.pcisecuritystandards.org/organization_info/index.php.
[16] Complaint at ¶ 41-42.
[17] Id. at ¶ 43-44.
[18] Id. at ¶ 37, 73, 74.
[19] Id. at ¶ 35, 78.
[20] Id. at ¶ 145-153.

(8) The government entity charged with implementing regulations may explain how companies should comply with their regulations. In this case, the Federal Trade Commission ("FTC") explained how a data security plan should be updated.[22] Check out the regulatory bodies' websites for possible guidance in interpreting their regulations.

(9) Consider investigating other litigation involving a potentially responsible IT provider. The plaintiffs in the Target case cited separate litigation involving the Fair and Accurate Credit Transaction Act (FACTA).[23] Plaintiffs cited expert testimony in the FACTA litigation in support of their claims in this data breach matter.

(10) Consider locating studies of the IT company's work. Plaintiffs in this case cited a study characterizing Target's IT systems as a "cost center" where they were trying to "drive down" costs.[24] This supported an argument that the system operators are more concerned about cost than safety.

(11) Companies that make filings with the U.S. Securities and Exchange Commission ("SEC") may include statements relevant to controlling standards. In this case, Target represented in its SEC filings that it had a data security incident detection program in place.[25]

(12) Discovery should explore a potentially responsible party's history of similar losses. The Trustwave complaint detailed multiple similar serious data breaches at Target since 2007.[26]

(13) Despite the numerous media reports of data breaches, they are preventable, at least according to plaintiffs in this case.[27] They cite seven specific actions that would have prevented this breach. If true, plaintiffs have provided a good example of how to establish that inadequate IT security measures caused a breach.

(14) Categories of damages caused by a data breach may be extensive and numerous. Plaintiffs in the Trustwave case claimed expenses, absorption of fraudulent charges, "business destruction, lost profits and/or lost business opportunities."[28] While there may be limits on consequential damages such as the economic loss doctrine, far-reaching damages due to data breach are worth exploring.

(15) Four of the eight counts in the complaint rely on Minnesota state law. Target is based in Minnesota.[29] Under Minnesota's Plastic Card Act, both defendants allegedly have strict liability for a data breach.[30] Consider whether states with jurisdiction have statutes applicable to the breach in question.[31]

---

[21] See id. at ¶ 153.
[22] Id. at ¶ 38.
[23] Id. at ¶ 77.
[24] Id. at ¶ 75.
[25] Id. at ¶ 37.
[26] Id. at ¶ 46-54.
[27] Id. at ¶ 87.
[28] Id. at ¶ 2.
[29] Id. at ¶ 8.
[30] Id. at ¶ 118.
[31] See also id. at ¶ 4.

(16) The complaint does not include a breach of contract claim. It appears there were no contracts between plaintiffs and the defendants. Even so, plaintiffs cited the contract between Target and MasterCard as proof of industry standards.[32]

(17) Possibly anticipating an argument by Target that the allegedly negligent actions were the responsibility of its IT provider and that Target should not be held liable for said actions because the IT provider is an independent contractor, plaintiffs cited warnings by a leading industry group of the "special risks" posed by outsourcing such IT work. That group also reminded retailers that they remained responsible for data protection even if they outsource the data protection work.[33]

In conclusion, the claim against Target and its IT company, Trustwave, may provide much useful material for a subrogating carrier's claim against a potentially responsible third party IT company that may have injured its insured.

[32] Id. at ¶ 78.
[33] Id. at ¶ 80.