Avoiding the Bullseye: CyberSecurity Lessons from the Target Litigation

David M. Furr, J.D.
Gray, Layton, Kersh, Solomon, Furr & Smith, P.A.

Special thanks goes to Rhett Butler, a 2018 candidate for J.D. from Wake Forest University School of Law for editing and properly citing this paper.

Traditional retail in the United States has had two distinct issues negatively affecting its survival in this decade. First, the proliferation of E-commerce companies has severely reduced the profitability of the traditional brick and mortar businesses as shoppers' habits are fundamentally changing. In the first four months of this year, nine retailers have filed for bankruptcy -- Payless Shoes, hhgregg, The Limited, RadioShack, BCBG, Wet Seal, Gormans, Eastern Outfitters, and Gander Mountain -- with the closing of hundreds of stores.[1] Many other retailers are shuttering stores at such a record pace that 2017 is being bannered as the year of retail bankruptcies.[2]

Second, retail has been particularly hard hit by cybersecurity breaches because of the wealth of Personal Identity Information (PII) collected and, unfortunately retained, by the retailers. The 2013 massive compromise of retail giant Target's systems has been litigated in the courts and subject to an extensive Multi-State Attorney-General Task Force action that has produced record payouts to plaintiffs.

The purpose of this paper is to use the Target litigation as a backdrop of the cybersecurity measures a business must have in place if it is to protect adequately the PII of its lifeblood --- the customers. While common tort and specific statutory theories serve as the foundation for these claims, the sophistication of the Plaintiff counsels' deep dive into the actual technology facts serve as an important road map to safe cybersecurity.

---

[1] Hayley Peterson, *'The dominoes are starting to fall': Retailers are going bankrupt at a staggering rate,* Business Insider, (Apr. 11, 2017), http://www.businessinsider.com/retailers-are-going-bankrupt-at-a-staggering-rate-2017-4.
[2] Id.

I. The Target Breach, By the Numbers

- **40 million** - the number of credit and debit cards stolen between November 27 and December 15, 2013
- **70 million** - the number of records stolen that included the name, address and email address of Target shoppers
- **46** - the percentage drop in profits at Target in the fourth quarter of 2013, compared with the year before
- **200 million** - estimated dollar costs to the credit unions and community banks for reissuing 21.8 million cards -- about half the total stolen
- **0** -- the number of people in Chief Information Security Officer (CISO) or Chief Security Officer (CSO) jobs at Target
- **$18 - $35.70** - the median price range per card stolen from Target and resold on the international black market, reaping an estimated $53.7 million in income
- **1 -** the resignation of the CEO[3]
- **$252 million -** costs associated with data breach through 2014[4]

II. Class Action Litigation and Multi-State Attorney-General Investigation

A class action was filed on behalf of consumers, which settled in 2015 for $10 million, paying individual victims up to $10,000 each in damages.[5]

---

[3] Brian Krebs, *Email Attack on Vendor Set Up Breach at Target,* Krebs on Security Blog, (Feb. 12, 2014). http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

[4] Kevin McGinty, *Target Data Breach Price Tag: $252 Million and Counting,* Mintz Levin Blog, (Feb. 26, 2015). https://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting/.

[5] *Target will pay $10 million to settle lawsuit from data breach,* Fortune Magizine (Mar. 19, 2015) http://fortune.com/2015/03/19/target-10-million-settle-data-breach/.

A Multi-State Attorney-General Task Force (47 states) recently concluded their investigation with the largest settlement achieved to date of $18.5 million for a cybersecurity breach.[6] North Carolina Attorney-General, Josh Stein, was quoted as saying "retailers must make the safety of their customers a priority."[7] The settlement requires Target to employ a CISO, to hire an independently-qualified third party to conduct a comprehensive security assessment, to maintain and support software on its network, to maintain appropriate encryption policies for PII, to segment its cardholder data environment from the rest of its network, to undertake steps to control access to its network (including password rotation and multi-factor authentification).[8]

Another class action, which is the subject of this paper, was filed by multiple financial institutions to recover massive costs to recover fraud losses and card reissuance expenses after customers used the cards at Target.[9] A published Memorandum and Order regarding Defendant's Motion to Dismiss was rendered on December 2, 2014.[10] Target ultimately settled this Class Action by depositing $39,357,939.38 into a Settlement Fund to be divided $20,250,000 into a Settlement Escrow account and $19,107,939.38 to MasterCard's Account Data Compromise

[6] Press Release, Eric Schneiderman, New York State Attorney General (May 23, 2017) https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over.
[7] *Target data breach leads to record settlement with 47 states, including N.C.,* Charlotte Business Journal (May 24, 2017), http://www.bizjournals.com/charlotte/news/2017/05/24/target-date-breach-leads -to-record-settlement-with.html.
[8] Id.
[9] Brief of Plaintiff, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (2014) (No. 14-2522).
[10] In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. Dec. 18, 2014) (No. 14-2522).

program.[11] Additionally, $20 million was awarded for attorney fees, reimbursement of expenses and service payments.[12]

III. The Motion to Dismiss the Consolidated Amended Class Action Complaint in the Financial Institution Cases

The Court's response as well as the Plaintiffs' Memorandum of Law[13] provides an excellent roadmap to litigate responsibility in cybersecurity breaches across most sectors. Generally, Defendant's briefs inexplicably fail to address facts and rely on whether certain legal principles apply or not. Plaintiffs, on the other hand, dove into the facts and technology to substantiate four claims: (i) negligence in failing to provide sufficient security to prevent the hackers from accessing customer data; (ii) violation of Minnesota Plastic Security Card Act, (iii) negligence per se, and (iv) negligent misrepresentation by omission due to Defendant's failure to inform Plaintiffs of its insufficient security.[14] Most of the Court's discussion and the Plaintiff's briefs focus on the first claim of negligence and facts in support thereof. While the other claims appear

[11] *Target Data Breach Settlement,* FAQ #4 (https://www.targetbanksettlement.com/FrequentlyAsked Questions#q4. Target also previously settled with Visa for $67 million to resolve claims made by Visa Card issuing banks under Visa's card resolution process. (Kevin McGinty, *Target Data Breach Price Tag: $252 Million and Counting,* Mintz Levin Blog, (Feb. 26, 2015). https://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting/.)

[12] Judgment in Civil Case, 14-md-2522 PAM (May 13, 2016).

[13] Memorandum of Law in Support of Financial Institution Plaintiffs' Motion for Final Approval of Class Action Settlement, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. Dec. 18, 2014) (No. 14-2522).

[14] In re: Target, 66 F. Supp. 3d 1154.

meritorious[15], specifically this paper focuses on the facts and law surrounding the negligence claim.

A. Negligence in Failing to Provide Sufficient Security to Prevent Hackers from Accessing Customer Data

Under Minnesota law, a claim of negligence requires a Plaintiff to allege four elements: duty, breach, causation and injury.[16]

i. Duty.

Under Minnesota law, a duty to act with reasonable care for the protection of others exists when a party's own conduct creates a foreseeable risk of injury to a foreseeable plaintiff.[17] Plaintiff's counsel argued compellingly a straightforward negligence case by showing that Target's own conduct in failing to maintain appropriate data security measures and disabling others created a foreseeable risk of harm to Plaintiffs, who were a foreseeable victim of that harm.[18] For the purpose of denying this Motion to Dismiss, the Court found the allegations

[15] The negligent omission claim was dismissed by the Court for failure to plead sufficient reliance on illegal omission. Nevertheless, the court provided that Plaintiffs may file an amended complaint within 30 days. Id. at 6.
[16] In re: Target, 66 F. Supp. 3d 1154.
[17] Id.
[18] Id.

sufficiently pled that Target was solely able and solely responsible to safeguard its and the Plaintiff's customers' data.[19]

ii. Bad Facts Doom Target.

Sometime in late September or October of 2013, third party hackers obtained unfettered access to Target's network through a third-party vendor, Fazio Mechanical, a heating, air conditioning and refrigeration firm in Sharpsburg, Pennsylvania. Apparently, Fazio itself was the subject of a random email phishing campaign.[20]

On November 15, 2013, the hackers uploaded card-stealing malware[21] onto Target's network that infiltrated most point-of-sale (POS) systems (in-store cash registers) by November 30.[22] Hackers also installed exfiltration malware, designed to store data on Target's own system, then move it several days later to the hacker's own systems in Russia.[23] From December 2-15, card data was collected as customers paid at the POS. Data was stored up to six (6) days on

[19] In re: Target, 66 F. Supp. 3d 1154, 1309. The Court also determined that with the plausible allegations of the existence of a duty, there could be no doubt that plaintiffs plausibly alleged that Target breached that duty by failing to safeguard Plaintiff's customers' information. Inexplicably Target counsel never challenged the allegations of causation and damages. Defendant counsel relied heavily on the general lack of a duty of care.
[20] Brian Krebs, *Email Attack on Vendor Set Up Breach at Target,* Krebs on Security Blog, (Feb. 12, 2014). http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.
[21] Malware known as TROJAN.POSRAM, a customized variant of BlackPOS malware had become easily available on the DarkWeb. At the time of discovery TROJAN.POSRAM had a zero percent detection rate among anti-virus vendors.
[22] Brief of Plaintiff, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (2014) (No. 14-2522).
[23] Id.

the Target network then exfiltrated. Despite numerous notifications by various parties that something bad might be happening, Target finally acknowledged the breach on December 19, 2013.[24] For almost two and one-half weeks in December, financial institutions' card data was being sold on the DarkWeb.[25] Credit card information of over 40 million customers along with PII of over 70 million customers had been exfiltrated.[26]

iii. Negligence Standard Applied by Court

The Court examined the following factors when determining whether a defendant owed a duty of care in a general negligence case: (i) the foreseeability of harm to a plaintiff, (ii) the connection between a defendant's conduct and the injury suffered, (iii) the moral blame attached to the defendant's conduct, (iv) the policy of preventing future harm, and (v) the burden to the defendant and community of imposing a duty to exercise care with resulting liability for a breach.[27] Despite this ruling being only as to a Motion to Dismiss, the Court found "Target played a key role in allowing the harm to occur."[28]

[24] Id.
[25] Id. at p.7.
[26] Brian Krebs, *Email Attack on Vendor Set Up Breach at Target,* Krebs on Security Blog, (Feb. 12, 2014). http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.
[27] In re: Target Corporation Customer Data Security Breach Litig., 64 F. Supp. 3d 1304; 2014 U.S. Dist. LEXIS 167802.
[28] Id at *1309.

B. General Failure by Target to Apply Any Fundamental Cybersecurity Principles to Avoid Negligent Conduct.

The Plaintiff's counsel provided very in-depth technical analysis of the failures of the Target network to suppress this attack. Despite the fact that the attack was unprecedented in the scope and scale of the operation, especially over an extended period, Target provided little defense for its lack of security.[29]

i. Target ignored multiple notices by insiders and by third parties that it was vulnerable or that it was being breached.

- In early to mid-2013, VISA issued alerts directly to Target about potential attacks using RAM-Scraper malware to extract full magnetic stripe data, along with specific measures to combat breaches similar to what hit in December.[30]
- In September 2013, Target's own security staff raised perceived vulnerabilities in Target's POS systems.[31]

[29] Defense counsel could easily have raised that FireEye alert was only with regarding to "binary malware", a generic alert with almost no detail. Counsel could also have raised the fact that Target was bombarded by hundreds of alerts per day, making it extremely tough to have singled out a thread that particularly malicious. Jim Finkle and Susan Heavey, *Target says it declined to act on early alert of cyber breach,* (Mar. 13, 2014, 6:39 PM), http://www.reuters.com/article/us-target-breach-idUSBREA2C14F20140313.

[30] Brief of Plaintiff, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (2014) (No. 14-2522).

[31] Of course, we now know, Target had no CISO to deal with security issues raised. Brian Krebs, *Email Attack on Vendor Set Up Breach at Target,* Krebs on Security Blog, (Feb. 12, 2014). http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

- On both November 30 and December 2, Target's advanced intrusion detection system sold by FireEye identified and notified Target of the malware.[32]
- On December 11, a Target employee noticed and reported suspicious activity.[33]
- On December 12, the Justice Department notified Target of the breach.[34]
- On December 19, Target finally acknowledged publicly the breach.

ii. Improper Defense Application.

Notably Target hired FireEye, a renowned intrusion detection company, to update its computer security with state-of-the-art malware detection, and, more importantly, an automatic malware deletion function.[35] The latter function could have prevented the breach, but Target inexplicably turned it off. Repeatedly in the published opinion, the Court was influenced by this overt act.[36] [37]

[32] Brief of Plaintiff, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (2014) (No. 14-2522).
[33] Id.
[34] Target only begins to purge the malware on December 15th, 2014, three days after notice from the Justice Department.
[35] Id.
[36] In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. Dec. 18, 2014) (No. 14-2522).
[37] Notably, the Defendant's counsel never focused on an alleged well-known fact by experts that the "vast majority of FireEye's customers turn off that functionality (malware deletion) because it is known for incorrectly flagging data as malware, which can halt email Web traffic for business owners. While FireEye is cutting edge, it takes love, care and feeding." Jim Finkle and Susan Heavey, *Target says it declined to act on early alert of cyber breach,* (Mar. 13, 2014, 6:39 PM), http://www.reuters.com/article/us-target-breach-idUSBREA2C14F20140313, quoting Shane Shook, Cylance, and John Strand, Black Hill Information Security.

iii. Failure to Comply with Minnesota Plastic Card Security Act (the Act).

The Court was persuaded by Target's failure to implement data retention policies, particularly as proscribed by the Minnesota Plastic Card Security Act.[38] The Act states that,

> No person or entity conducting business in Minnesota that accepts a[] [credit or debit cards] in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.[39]

Information from card transactions was routinely stored for two-to-three months after such transactions occurred.[40] Even though the Act violation lodged as a separate claim by Plaintiffs, the Court is influenced by the Act application in the negligence claim, when it states that "imposing a duty on Target in this case will aid Minnesota's policy of punishing companies that do not secure consumers' credit and debit card information."[41]

[38] In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154, 1312 (D. Minn. Dec. 18, 2014) (No. 14-2522).
[39] Id.
[40] Brief of Plaintiff, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (2014) (No. 14-2522).
[41] Defense counsel inadequately countered this claim with (i) the Act only applies to business transactions that take place in Minnesota, and (ii) the Act covers data retention which does not apply because data was stolen in real time, hence never retained. The Court is wholly unpersuaded by either of these

iv. Failure to Segment its Network

While not a focus of the Court's opinion, Plaintiffs allege Target's failure to segment its network. As we now know, the initial intrusion was via Fazio Mechanical, itself a victim of an email phishing campaign.[42] A basic premise of segmentation is to isolate sensitive information from the general network, using the concept of limited to zero trust to only allow content to be accessed by limited and identifiable set of users, through a well-defined set of applications, blocking everything else. In modern defense strategy, no POS machine with sensitive customer payment data should be able to connect to the general network and allow data exfiltration.

v. Failure to require two- or multi-factor authentification or an Encryption Policy

While not a focus of the Court's opinion, the Plaintiffs allege failure to require two- or multi-factor authentification.[43] The Multi-State Attorney General Task Force also focused on the lack of any encryption policies.[44] Had Target assigned assets handling payment to a segmented security zone and had Target required authentification for access only through specific and identifiable users

defenses. In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154, 1158 (D. Minn. Dec. 18, 2014) (No. 14-2522).

[42] Brief of Plaintiff, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (2014) (No. 14-2522).

[43] Id.

[44] *Target data breach leads to record settlement with 47 states, including N.C.,* Charlotte Business Journal (May 24, 2017), http://www.bizjournals.com/charlotte/news/2017/05/24/target-date-breach-leads - to-record-settlement-with.html.

utilizing basic encryption within the zone, the breath and scope of this breach would have been much more unlikely, if not impossible, to have occurred.

vi. Failure to Adopt Next Generation Firewalls.

While not a focus of the Court's opinion, the Plaintiffs allege failure to erect strong firewalls.[45] Along with segmentation and multi-factor authentification, employment of next generation firewalls would have forced authorized traffic to flow from POS-related systems to well-defined security zones, such as payment processors. With these controls in place, all outbound and inbound communication outside of this strict set of controlled access, user and applications would be implicitly denied, greatly limiting the attacker's ability to pivot towards sensitive assets from the initial compromise or exfiltrate data from the POS. Moreover, a next-generation firewall that incorporates prevention technology and sandboxing should have analyzed and automatically deleted suspicious files crossing the network, including the Trojan.POSRAM malware.[46]

vii. Failure to Require Vendors to Monitor the Integrity of Their Files.

[45] Brief of Plaintiff, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154 (2014) (No. 14-2522).
[46] POS-forward malware was first noticed in 2010.

While not a focus of the Court, Plaintiffs also allege that Target failed to require its vendors to monitor the integrity of their files.[47] A robust supply chain ecosystem provides significant competitive advantages for companies that strategically and securely source from vendors or utilize vendor services, wherever they may be. Modern cybersecurity requires that all contracts with vendors be both modified to require vendor security certification and indemnity for failure to do so.[48]

Conclusion

To rule in favor of the Plaintiff Financial Institutions in the Motion to Dismiss, the Court analyzes only a few of the "bad facts" in depth that force Defendant into settlement posture. Plaintiff's counsel deeply dove into the abject failure of Target to secure properly its network from a devastating intrusion and marshaled those facts and technology to support applicable legal theories. While the few facts analyzed are important, the wealth of other "bad facts" could just as easily have doomed Target.[49] Regardless the Plaintiff's litigation briefs and the opinion provide an excellent roadmap to modern cybersecurity standards and need for all businesses (not just retail) to protect the critical PII of their lifeblood -- their customers.[50]

[47] Brief of Plaintiff, In re: Target Corporation Customer Data Security Breach Litig., 66 F. Supp. 3d 1154; (2014) (No. 14-2522).
[48] The author can only speculate the value of an indemnify from a small HVAC company.
[49] Per this author, Defendant counsel's concentration on technical legal applications is unfortunate, but perhaps the only perceived hope in light of the overwhelming lack of network security.
[50] The same analysis can be utilized for personal healthcare information (PHI), customer information (CI), and even intellectual property (IP) protections. The standards litigated in this case are quite agnostic.

The two lessons of the Target litigation are that organizations of every size can make significant gains in improving their security posture by first identifying their most valuable data and building layers of defense around it to protect its confidentiality, integrity and availability. Without knowledge of which assets are most critical to protect, organizations tend to protect everything equally, which may in fact increase costs and provide less protection.

After the most critical data is identified, segmenting the network into security zones guarded by next generation firewalls greatly reduces the likelihood of a compromise spreading and increases visibility of traffic across the network. As we saw in the Target intrusion, the lack of any network segmentation and next generation firewall protection allowed the intruders to access all data indiscriminately once inside the network in an unprecedented attack in both depth and breath.

Every organization should adopt these two important principles into an overall security strategy: (i) layers of defense around the most critical data and (ii) network segmentation guarded by next generation firewalls. While larger organizations can employ and manage the technologies discussed in this paper, smaller organizations can now rely on managed services from a security partner to provide “best-in-class” technology and resources required to protect and monitor their most valuable assets at very reasonable costs.

Traditional retailers are overwhelmed by external forces that are forcing a complete reconsideration of how to best influence the consumer. Proper

cybersecurity will not drive their marketing; however, failure to defend can cause extraordinary unanticipated costs and permanent (if not fatal) brand damage.