Target, Negligence, Chips, and Chickens

By JESSE D. GOSSETT*

SHOPPING ON BLACK FRIDAY. It's almost as American as baseball and apple pie. But during the 2013 holiday season, over forty million U.S. citizens experienced what is increasingly becoming a uniquely American problem: face-to-face ("FTF") credit card fraud.[1] FTF credit card fraud occurs when a consumer's credit card magnetic stripe ("magstripe") is swiped through a merchant's card reader.[2] The fraud occurs when someone intercepts the information somewhere along the way. In the case of Target's December 2013 data breach,[3] the interception of credit and debit card information[4] happened using a so-called memory parsing malware at the Point of Sale ("POS").[5] But this is not the only interception method. Nearly ten years ago, fraudsters used wireless technology to access the unencrypted network of Marshall's, which allowed them to access at least forty-five million credit card numbers.[6] Or, the theft can be as seemingly low tech as so-called skimming where the fraudster places a secondary card

[*] J.D., Cum Laude, University of San Francisco, 2014. Chartered Financial Analyst and Certified Financial Planner. Editor-in-Chief, USF Law Review, Volume 48. Thank you to Pareesa Ashabi and Jennifer L. Sta.Ana and the entire USF Law Review Volume 49 Board for making the dream of an online law review a reality.

[1] Jim Finkle & Mark Hosenball, *Exclusive: FBI Warns Retailers to Expect More Credit Card Breaches*, REUTERS (Jan. 23, 2014), http://www.reuters.com/assets/print?aid=USBREA0M1UF20140123 ("The [Target] attack ran undetected for 19 days during the busy holiday shopping season and resulted in the theft of about 40 million credit and debit card records.").

[2] *See* Douglas King, *Chip-and-Pin: Success and Challenges in Reducing Fraud* 2, (Federal Reserve Bank of Atlanta, Retail Payments Risk Forum Working Paper, Jan. 2012), *available at* http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf.

[3] *Data Breach FAQ*, TARGET, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888 (last visited Sept. 24, 2014) ("In mid-December 2013, [Target] learned criminals forced their way into our system, gaining access to guest credit and debit card information.").

[4] *Id.*

[5] *See* Finkle & Hosenball, *supra* note 1.

[6] Joseph Pereira, *How Credit-Card Data Went Out Wireless Door*, WALL ST. J. (May 4, 2007, 12:01 AM), http:// online.wsj.com/news/articles/SB117824446226991797.

reader on an ATM or gas pump, or the waiter you handed your credit card to at lunch swipes it through a device on his smart phone before giving it back to you.[7] What all of these frauds have in common is they take advantage of a serious flaw in the credit card payment processing system in the United States. Namely, our credit card system relies on forty-year-old magstripe technology.[8]

Magstripes contain all of the information necessary to effect a transaction. If a person can obtain that information, that person can easily manufacture a fake card and use it for her own fraudulent transactions. [9] The primary reason this is true is because the information on a magstripe is static[10] so, once it is obtained, it can be used over and over until the cardholder notices the fraudulent transactions and cancels his card. However, an alternative to magstripes called EMV chip-and-PIN has existed for well over a decade.[11] Cards with this technology have a small chip embedded in the card on the left-hand side. The credit card information on the chip is highly encrypted, and the encryption is dynamic making it nearly impossible to decode.[12] The security is further enhanced by the need of the cardholder to enter a PIN to verify herself as the owner of the card.[13] Rolled out on a national level in the U.K. in 2002,[14] chip-and-PIN has reduced domestic fraud in that country by over 34% and FTF fraud

[7] Joe Green, *Credit Card 'Skimming' a Real Danger, Secret Service Officials Warn*, S. JERSEY TIMES (Oct. 14, 2013, 11:36 AM), http://blog.nj.com/gloucestercounty_impact/print.html?entry=/2013/10/creditdebit_card_skimming_a_real_danger_south_jersey_secret_service_officials_warn.html.

[8] *DPD Chronology*, IBM, http://www-03.ibm.com/ibm/history/exhibits/dpd50/dpd50_chronology4.html (last visited Sept. 23, 2014) ("On February 24, the IBM Information Records Division establishes a Magnetic Credit Card Service Center to support the Data Processing Division's new IBM 2730-1 transaction validation terminal."); Howard Schneider, Hayley Tsukayama & Amrita Jayakumar, *U.S. Credit Cards, Chipless and Magnetized, Lure Global Fraudsters*, WASH. POST (Jan. 21, 2014), http://www.washingtonpost.com/business/economy/us-credit-cards-chipless-and-magnetized-lure-global-fraudsters/2014/01/21/6edd171e-7df3-11e3-9556-4a4bf7bcbd84_story.html (identifying magnetic stripe usage as putting U.S. consumers at risk for years to come).

[9] *FAQ: EMV Chip Card Technology*, CHASE PAYMENTECH, https://www.chasepaymentech.com/faq_emv_chip_card_technology.html (last visited Sept. 24, 2014) ("Consequently, data from a traditional magstripe card can be easily copied (skimmed) with a simple and inexpensive card reading device – enabling criminals to reproduce counterfeit cards for use in both the retail and the CNP environment.").

[10] King, *supra* note 2.

[11] *Id.* at 5 ("Following several successful chip-and-PIN trials in the mid- to late-1990s, the [U.K.] decided on a national rollout of EMV chip-and-PIN in 2002.").

[12] *Id.* at 2.

[13] *Id.*

[14] *Id.* at 5.

by 69%.[15] This technology is also widely used in Europe, Canada, and Australia, and has dramatically reduced domestic FTF fraud by significant percentages in these regions as well.[16] In fact, the United States is the only developed country that has not embraced this technology.[17] This makes the United States the last great target for international fraudsters,[18] which is why this is increasingly becoming a unique problem for U.S. citizens.

Some credit card issuers have started issuing chip-and-PIN enabled cards in the U.S.[19] However, for all intents and purposes, the chip-level of security is wasted because no merchants have chip-enabled terminals.[20] Ironically, I can only obtain this high-level of security by traveling overseas. Why is the credit card industry slow to adopt this standard? The answer can be articulated in one word: money. It will cost an estimated eight billion dollars to convert the U.S. credit card system to chip-and-PIN processing.[21] While the costs of fraudulent transactions are typically borne by the issuing banks (for example, card-not-present ("CNP") instances[22] are the merchant's responsibility), these costs are usually transferred to the card customers and merchants through higher fees.[23] In essence, the only apparent motivation for card companies to adopt this standard in the United States is the threat consumers may become fearful of using their cards and revert to a cash-based society. As mentioned, card companies are beginning to adopt this standard, but this is primarily to accommodate customers that travel internationally.

While credit card companies have yet to fully embrace alternatives to the magstripe system, other companies have begun to step in and offer

[15] *Id.* at 6.

[16] *Id.* at 4 ("According to data from the UK Payments Administration, EMV chip-and-PIN has been successful at reducing certain types of card fraud, especially domestic counterfeit and lost or stolen card fraud. Total card fraud in the UK began declining in 2005 as the chip-and-PIN movement gained traction."); *Id.* at 14 ("Although the national roll-out of chip-and-PIN did not begin until late 2008, similar fraud migration trends experienced in other chip-and-PIN markets are appearing in Canada."); *Id.* at 17 ("With migration to EMV chip-and-PIN in Australia still in its early stages, data from the APCA is already showing similar patterns of fraud trends observed in more mature chip-and-PIN markets.").

[17] *See id.* at 1.

[18] *Id.*

[19] *See id.* at 3.

[20] *See id.* at 4.

[21] Schneider, Tsukayama & Jayakumar, *supra* note 8.

[22] A "CNP" transaction is completed when the cardholder is not physically present to hand the credit card to the seller. *E-Commerce Glossary*, 2CHECKOUT, https://www.2checkout.com/ecommerce-glossary/card-not-present (last visited Sept. 24, 2014).

[23] Lydia Segal, Benjamin Ngugi & Jafar Mana, *Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem*, 16 FORDHAM J. CORP. & FIN. L. 743, 749 (2011).

alternatives. Apple's new iPhone 6, which launched earlier this month on September 19, incorporates the company's new Apple Pay system.[24] Apple CEO Tim Cook, touts this system as being safer than the "'outdated and vulnerable magnetic-stripe.'"[25] Whether this system really is safer than the chip-and-PIN system, or even the magstripe system, remains to be seen. While Apple's CEO certainly thinks so, others disagree.[26] Even if Apple Pay is not more secure, Apple's step into the "burgeoning" field of mobile payment systems prompted the support of at least one credit card company.[27] While not a move toward the chip-and-PIN system, shortly after Apple's announcement, Visa announced it would be partnering with Apple to make its Token Pay system compatible with the device.[28] (Visa's eponymous tokens are stored on the mobile device and replace the payment information on the physical cards.)[29]

In either event, Apple may have an even greater problem than the security of its payment system, at least according to one academic. Georgetown law professor Adam Levitin believes Apple is now a service provider under the Consumer Financial Protection Act and therefore subject to its financial regulations.[30] Apple Pay works by creating a Device Account Number, which is assigned, encrypted, and stored on a special chip on the iPhone 6.[31] When a purchase is made, "the Device Account Number, along with a transaction-specific dynamic security code, is used to process your payment."[32] This is known as "tokenization."[33] Levitin believes Apple's active role in determining what information is sent makes

[24] John Leyden, *Apple's New iPhone 6 Vulnerable to Last Year's TouchID Fingerprint Hack*, THE REGISTER (Sept. 23, 2014), http://www.theregister.co.uk/2014/09/23/iphone_6_still_vulnerable_to_touchid_fingerprint_hack/.

[25] Adam Clark Estes, *How Safe Can Apple Pay Really Be?*, GIZMODO (Sept. 10, 2014, 4:10 PM), http://gizmodo.com/how-safe-can-apple-pay-really-be-1633065822.

[26] *Id.* (pointing out Apple's less than perfect history of security breaches and the vulnerabilities of transferring the payment data via near field communication ("NFC")).

[27] Samantha Sharf, *As Apple Pay Hits, Visa Signals Hopes To Be Mobile Payment Player*, FORBES (Sept. 18, 2014 10:09 AM), http://www.forbes.com/sites/samanthasharf/2014/09/18/as-apple-pay-hits-visa-signals-hopes-to-be-mobile-payment-player/.

[28] *Id.*

[29] *See infra* text accompanying note 33.

[30] Adam Levitin, *Apple Pay and the CFPB*, CREDIT SLIPS (Sept. 10, 2014, 10:56 PM), http://www.creditslips.org/creditslips/2014/09/apple-pay-and-the-cfpb.html.

[31] *Apple Pay*, APPLE, https://www.apple.com/iphone-6/apple-pay/ (last visited Sept. 18, 2014).

[32] *Id.*

[33] Darrell Delamaide, *Delamaide: Apple Pay May Test Regulators*, USA TODAY (Sept. 16, 2014, 8:44 PM), http://www.usatoday.com/story/money/business/2014/09/16/delamaide/15743653/.

Apple a service provider under the Consumer Financial Protection Act,[34] not merely a common carrier.[35]

Aside from being forced to move to other payment systems by competitors like Apple, is there another way to motivate the credit card industry to get its act together and adopt better security standards without consumers threatening to ditch cards and barter chickens for goods and services? There very well may be—at least in California (and states with similar privacy protections). The California Constitution makes privacy an inalienable right,[36] and breaches of that privacy are actionable in tort.[37] To show an invasion of privacy, a plaintiff must first allege a specific, legally protected privacy interest.[38] The recognized privacy interest at issue here is informational privacy (for example, interest in precluding the dissemination or misuse of sensitive and confidential information). The next element is that there is a reasonable expectation of privacy.[39] Finally, actionable invasions of privacy must be sufficiently serious in nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.[40]

In the case of these credit card frauds, clearly those perpetrating the fraud have violated Californian's privacy laws. But what about the credit card companies? First, it should be fairly obvious that credit card customers have an interest in precluding the dissemination and misuse of their credit card information. Second, the California Financial Information Privacy Act ("CFIPA")[41] makes it unlawful to "sell, share, transfer, or otherwise disclose nonpublic personal information to or with nonaffiliated third parties" without the express consent of the consumer.[42] Further, the CFIPA provides for liability and civil penalties—irrespective of the damages suffered by the consumer—for the *negligent* disclosure of nonpublic personal information.[43] Further, the California Supreme Court has very

[34] "Covered persons" under the Consumer Financial Protection Act includes "any person that engages in offering or providing a consumer financial product or service." 12 U.S.C. § 5481(6) (2010).

[35] Delamaide, *supra* note 33.

[36] CAL. CONST. art. I, § 1.

[37] Hill v. NCAA, 865 P.2d 633, 647 (Cal. 1994).

[38] *Id.* at 654.

[39] *Id.* at 655.

[40] *Id.*

[41] CAL. FIN. CODE §§ 4050–4060 (West 1999 & Supp. 2013).

[42] CAL. FIN. CODE § 4052.5 (West 1999).

[43] CAL. FIN. CODE § 4057 (West 1999) (allowing penalties up to $2,500 per violation or up to $500,000 if more than one consumer is affected and double civil penalties if the violation results in identify theft of the consumer).

clearly stated that "[a] credit card holder would reasonably expect" confidentiality in his credit card transactions.[44] Clearly, the CFIPA and the California Supreme Court have articulated what most of us already reasonably expect: privacy in our financial information. Finally, the invasion of privacy must be serious to be actionable.[45] Here, the extent and gravity of the invasion is taken into consideration.[46] It is hard to imagine the theft of over forty million people's personal information is not serious. It is presumed the perpetrators are overseas, and massive amounts of identity theft could be occurring right now. Violations of the CFIPA and California Constitution seem highly plausible.

Not only is this an actionable privacy violation (remedies for which are actual damages and emotional distress), but also negligence. Clearly the CFIPA places a duty on financial institutions to safeguard their customers' financial information.[47] The question is whether that duty was breached. This brings the picture full circle. The credit card industry has had knowledge of the superiority of chip-and-PIN technology over magstripes for several years[48] but has chosen not to implement it. The industry made a calculated decision to prefer their profits to the risk of subjecting their customers to credit card fraud and identity theft. Perhaps a class-action suit on behalf of California credit card customers would help the credit card industry move a little faster in adopting chip-and-PIN in the United States. Otherwise, we might revert back to bartering chickens.

[44] People v. Blair, 602 P.2d 738, 746 (Cal. 1979).

[45] Hill v. NCAA, 865 P.2d 633, 655 (Cal. 1994).

[46] *Id.*

[47] § 4052.5.

[48] *See* King, *supra* note 2, at 5, 10 (highlighting success of chip-and-PIN in the U.K. in the mid- to late-1990s and an 89% reduction in France by 1995).