International Journal of Innovation Scientific Research and Review
Vol. 03, Issue, 05, pp.1199-1206, May, 2021
Available online at http://www.journalijisr.com

IJISRR

Research Article

ISSN: 2582-6131

IS IDENTITY THEFT USING SKIMMERS A SERIOUS THREAT OR A MINOR INCONVENIENCE?

*** Donald L. Buresh, Ph.D., J.D., LL.M.**

Morgan State University LoganSquareDon@sbcglobal.net

Received 17th March 2021; Accepted 18th April 2021; Published online 29th May 2021

ABSTRACT

The purpose of this article is to attempt to answer the question of whether skimmers and identify theft are a serious threat or a minor inconvenience. The issue under consideration is whether skimming can be construed to be a victimless crime or a crime where the damages are insufficient for police departments to take seriously. The essay describes the author's experience when his ATM car was skimmed and his identity was stolen. The paper proceeds to discuss some of the technical aspects of skimming and provide a brief history of the technology. The issue is stated, followed by examining the structural characteristics, the psychosocial qualities, technological procedures, mitigation issues, and societal goals and objectives in preventing the crime from occurring. Several alternatives are presented, where it is argued that society currently has sufficient safeguards in place, making additional precautions unnecessary. The article concludes by highlights some of the consequences of combating skimming.

Keywords: ATM Cards, Credit Cards, Debit Cards, Identity Theft, Skimmers.

INTRODUCTION

The purpose of this article is to attempt to answer the question of whether skimmers and identify theft are a serious threat or a minor inconvenience. The issue under consideration is whether skimming can be construed to be a victimless crime or a crime where the damages are insufficient for police departments to take seriously. Based on the experience of the author, it appears that credit card skimming, although a federal crime, is not taken seriously by local law enforcement unless the number of instances is voluminous, in which case, federal, state, and local law enforcement may take notice.[1]

THE SKIMMING AND STEALING OF MY IDENTITY

On a bright and sunny day, a short time ago, I went shopping and paid bills. In the late morning, I came home and began my workday. I work at home. Around four o'clock in the afternoon, I received a telephone call from Fidelity Information Services,[2] asking me about the last five transactions that I had made with my automated teller machine (ATM) card. The person on the other end of the phone stated that the last three transactions were made in a town about fifty miles away. I explained to her that I had not been in that town for well over five years. She then asked me whether I was in possession of my ATM card. I looked in my wallet where I keep it. It was there alright. This individual asked me if I had lent out my ATM card to anyone. I said no. I have never given anyone my card, and I would never do that. I asked her what was going on. She stated that someone in that town fifty miles away was using my card to purchase gasoline and other goods. She said that Fidelity had canceled my ATM card because it was being used outside of my usual geographical area. I thanked her, saying that I would be going to my bank to report what happened and apply for a new card. My final question was to ask her how did this happen. She told me that my ATM information had been "skimmed."[3] Somewhere I had made a purchase where the machine that I had used contained an illegal device known as a "skimmer."[4] In the course of buying something, at a local store or on the Internet, my information had been stolen. The perpetrators then made a fake ATM card[5] where my information was illegally copied onto the magnetic stripe on the back of a new card.[6] The fake ATM card then came into the possession of the person who posed as me, purchasing gas and other goods at several different stores. If there was good news, it was that amount of money at risk was slightly less than one hundred dollars. I arrived at my bank about 30 minutes before it closed. I talked to my banker and shared with her the information that Fidelity had provided me. She was both understanding and thorough. At my request, she printed out all of the information regarding the transactions that had occurred in that town earlier that morning.[7] I signed some papers disavowing the three transactions and ordered a new ATM card. My banker said that the bank would reimburse me the money that I had lost and take approximately seven to ten business days to receive my new card.[8] I was annoyed because I was inconvenienced through no fault of my own. I took cash out of my checking account so that I could use it for the upcoming week. I felt violated because I had become comfortable using my ATM card over the last ten years. I had read about identity theft but never thought that it would happen to me. I thought that my ATM card was safe to

[1] Chanelle Bessette, How Serious a Crime Is Credit Card Theft and Fraud?, Nerd Wallet, (June 01, 2020), https://www.nerdwallet.com/article/credit-cards/credit-card-theft-fraud-serious-crime-penalty#:~:text=In%20addition%20to%20the%20identity,or%20other%20counterfeit%20access%20devices.&text="Minor%20offenses%20can%20result%20in,fraud%20can%20lead%20to%20prison."

[2] Fidelity Information Services, https://www.fisglobal.com/about-us/about-our-company. Fidelity Information Services is a global provider of financial technology solutions. The company is headquartered in Jacksonville, Florida and services more than 20,000 clients in 130 countries.

[3] Skimming, INVESTOPEDIA, (n.d.), http://www.investopedia.com/terms/s/skimming.asp?lgl=myfinance-layout-no-ads. Skimming is an electronic method of capturing a person's personal information that is contained on ATM or credit cards.

[4] Id. A skimmer is a small electronic device that scans an ATM or credit card, storing the data that is contained on the magnetic strip located on the back of the card. Skimming usually occurs while a person is conducting a legitimate business transaction.

[5] Brian Gardiner, How Anyone Can Fake an ATM and Steal Your Money, GIZMODO, (2010), http://gizmodo.com/5687689/how-anyone-can-fake-an-atm-and-steal-your-money.

[6] Id.

[7] While at my local bank gathering information about the crime, my banker printed out for me detailed information regarding three illegal transactions that occurred that day.

[8] My bank's policy was to reimburse customers who lost money from identity theft.

use.[9] I was wrong. I called the two businesses where the illegal purchases were made in an attempt to find the culprit who impersonated me. Both businesses were gas stations.[10] At the first gas station, the manager told me that the offender had used the fake card to purchase gasoline. I asked the gentleman whether the company had recorded the face of the customer. He said that the transaction had occurred at the pump, where there were no cameras.[11] I had better luck when I called the second gas station. It turned out that this individual, a young man in his early thirties, had gone into the store itself to pay for gas and buy some other things. The second gas station manager said that she had waited on this person herself and recorded the whole transaction. I felt relieved. Now, just maybe, the police could intervene, find this person, and arrest him, provided that he could be identified. After I came home from the bank, I called the police department in the town where the crime took place to file a complaint. The dispatcher told me that I would first have to file the complaint in the city where I lived, and then the police department in my town would fax the report to the police department in the city where the illegal transaction occurred.[12] I was pleased because it meant that I would not have to travel fifty miles to file the police report. It was dark now. I drove to the police department in my town and filed the complaint. I explained what had happened and gave the officer on duty a copy of the papers that I had received from my bank. The officer said that I should come by on Monday to pick up a copy of the complaint. I was content in the knowledge that the wheels of justice were turning. That night, I spent five or six hours on the Internet until two o'clock in the morning investigating what skimming was and how it was done. I discovered that there are three different types of machines used when skimming debit and credit cards. The first type of device is what is called an *attach-on*.[13] This device attaches to a card reader on the outside of the machine using glue or a magnet. The second type of skimmer is an *overlay*.[14] The skimmer overlays an ATM's keyboard or overlays a credit card reader at a grocery or convenience store. This type of skimmer can be easy to spot when the overlay hides some of the card reader's features, such as the light pen's plastic holder. When the overlay sits on top of a keypad to be used in conjunction with an ATM, the overlay typically looks like the real keypad, and it can be difficult to discover.[15] The last type of skimmer is the most insidious. It is an *insert*.[16] This kind of skimmer consists of a wafer-thin computer board inserted into the orifice where a person enters their credit card.[17] As the machine reads personal credit card information, the skimmer is also reading the information and storing it.[18] With this type of skimmer, it is impossible to see it from outside the machine. To determine whether an insert skimmer is present, a person must physically open the ATM machine and carefully examine the device for the skimmer[19]. For a customer, this is impossible. A customer does not have permission nor the ability to open a card reader and then check for a skimmer. This task is the exclusive responsibility of a company's employees and management.[20] In the intervening time that has gone by, my bank reimbursed me the money that was stolen from my bank account. I have heard nothing from the police departments in my town or the other town. I have also not heard anything from either of the gas stations. When I called the manager at the second gas station, this person had promised me that the business owner would call me the next day about this matter. I have yet to receive a call from the proprietor. Was the theft of my identity a victimless crime? Probably an insurance company or the bank reimbursed my account so that I did not lose my money.[21] However, the bank and the insurance company probably considered my reimbursement as the cost of doing business.[22] The culprit had the goods that he paid for with my fake debit card, making him in some respects a winner. Most likely, he will never be caught because most people in my position will not go to the trouble of reporting the crime to the police.[23] They may view the theft as a minor inconvenience. However, they will most likely report the crime to their bank to get their money back if they notice any discrepancies in their bank statements.[24] I want justice to be done, but then again, my loss was relatively small. In the end, I broke even. I was neither a winner nor a loser. My complaint will probably be stored away like most penny-ante crimes in a large file cabinet somewhere or in an obscure database.[25] Nothing will happen except that I will write this article about skimming. At the very least, this is how justice will be achieved. Other people will read this article, and maybe I will inspire one of my readers to take a similar action when their identity is stolen. I certainly hope so.

ALL ABOUT SKIMMERS

According to the Data Specialist Group, a company specializing in digital forensics, a skimmer is an electronic device that can intercept a person's data without being observed.[26] Skimmers typically have internal electronic memory and may be able to communicate wirelessly with a criminal.[27] Skimmers are usually found in places where many financial transactions occur, such as ATMs, gasoline stations, retail stores, and even medical facilities.[28] Here is how a skimmer works. Two components must work together to skim the data on an debit or credit card successfully. The skimmer must interact with a card reader so that when a person slides their card through the reader, the skimmer then scans the information on the magnet strip or the chip present on the card.[29] However, to use the information gathered, another device is needed to collect a person's PIN.[30] This can be achieved in several ways. First, a camera situated immediately above a keypad can record the buttons pressed by an

[9] Theo Thimou, Why You Should Never Use a Debit Card to Pay for Anything, CLARK.COM, (2017), http://clark.com/personal-finance-credit/5-more-places-you-should-never-use-debit-card/.
[10] Id.
[11] Gas Station Surveillance Systems, CCTV CAMERA PROS, (2017), https://www.cctvcamerapros.com/Gas-Station-Surveillance-s/226.htm.
[12] When speaking with the police department where the identity theft, I was informed that I should file the report with the police department where I live. The police department where I live would then fax their report to the police department where the incident occurred.
[13] Skimmers: Hi-Tech, Low Cost Data Breaches Affecting Small Businesses, DATA SPECIALIST GROUP, (n.d.), http://dataspecialistgroup.com/wp-content/uploads/2015/02/SkimmersII.pdf. Here, their PowerPoint provided detailed information about the various different types of skimmers.
[14] Id.
[15] Id.
[16] Id.
[17] Credit Card Skimmer Information for Motor Fuel Retailers, WISCONSIN BUREAU OF WEIGHTS AND MEASURES, (2016), https://datcp.wi.gov/Documents/CreditCardSkimmerInfoForRetailers.pdf. This web site contains a plethora of pictures with explanatory text showing actual skimmers that were found at Wisconsin gasoline stations.
[18] Id.
[19] Id.
[20] Id.
[21] Penny Crosman, Do Banks Need to Rethink Identity Protection Services?, AMERICAN BANKER, (2015), https://www.americanbanker.com/news/do-banks-need-to-rethink-identity-protection-services.
[22] Id.
[23] Seena Gressin, Most ID Theft Victims Don't Need a Police Report, FEDERAL TRADE COMMISSION: CONSUMER INFORMATION, (2017), https://www.consumer.ftc.gov/blog/most-id-theft-victims-dont-need-police-report.
[24] Id.
[25] Id.
[26] Skimmers: Hi-Tech, Low Cost Data Breaches Affecting Small Businesses, supra, note 12.
[27] Id.
[28] Id.
[29] LaToya Irby, How Credit Card Skimming Works, THE BALANCE, (2017), https://www.thebalance.com/how-credit-card-skimming-works-960773.
[30] Brian Krebs, All About Skimmers, KREBS ON SECURITY, (2017), https://krebsonsecurity.com/all-about-skimmers/.

individual using a card reader.[31] Second, a skimmer can consist of a fake keypad that records what buttons are pressed as they enter their personal identification number (PIN).[32] Of course, for this type of skimmer to work, the PIN must be conveyed to the actual keypad, usually by a plastic bubble filled with air that compresses as a person presses a button on a fake keypad.[33] The compressed air then depresses the appropriate key on the keypad, conveying the card reader's information. Another type of skimmer fits into the orifice where a person inserts their ATM or credit card.[34] This device is a thin piece of plastic that contains electronic readers that glean the information from the magnetic strip or the chip inside a card.[35] The skimmer must also allow the actual card reader to collect a person's information so that the transaction is successful. The individual is completely unaware that the information on their card has been stolen.[36] Again, the skimmers that are inserted into a card reader must also be able to collect a person's PIN so that the information gathered can be used effectively in other criminal activities. With devices that can be purchased at most electronic retail stores, individuals can make their skimmers.[37] Because gas pumps use a universal physical key that can be purchased online, a criminal can open up a gasoline pump and insert a skimmer in a matter of seconds.[38] These skimmers consist of a ribbon cable and two multi-pin connectors, where the skimmer and it cable intercedes with the gas pump.[39] Another type of skimmer inserted into a credit card reader in a gas pump is made out of thin metal or plastic.[40] It is put in a different position within a card reader and is entirely hidden from a consumer looking at the front of an ATM.[41] The bad news is that the skimmer fits so far into a card reader that it is nearly impossible to detect them or jam them using current technology.[42] A skimmer can be installed any time in a day, but because few people are awake late at night and because third-shift personnel are not as diligent as the day-time staff, the hours after midnight or early morning are the preferred times to install a skimmer.[43] Once the debit or credit card information has been skimmed, the criminal needs to gather the data. If a criminal collects the information from an ATM card, a criminal also needs to know the PIN associated with the card to use the information.[44] There are several ways to obtain this information. A criminal may install a camera at a gas pump that records the buttons that a customer pushes when making a transaction.[45] Suppose a criminal employs a device that overlays a numeric keypad. In that case, the overlay can quickly capture the PIN while at the same time permitting the transaction to occur without a customer knowing that his or her card has been skimmed.[46] Suppose the information contained on the magnetic stripe is encrypted. In that case, the company that issued the card employs a universal public key that decrypts the data. A criminal is in possession of that key. It is a simple task to decode the magnetic stripe's information, thereby harvesting the PIN.[47] With the PIN in hand, a fake credit card can be made with the customer's PIN, which the criminal knows. A criminal can physically retrieve a skimmer or instruct the skimmer to transmit the skimmed information to a cell phone or another computing device.[48] If a skimmer must be manually retrieved, a criminal is exposing himself or herself to the risk of being caught.[49] A criminal manually retrieves a skimmer because the device contains neither the hardware nor software to transmit the information upon request.[50] In contrast, the more sophisticated skimmers do not need batteries because they draw power from machines reading ATM or credit cards.[51] With this new technology, a criminal, while being relatively close to a card reader, transmits a signal to the skimmer ordering the device to send the data that it has previously collected.[52] This fact is rather important because it is difficult for law enforcement to determine who is skimming debit or credit cards. When skimmers used batteries, they incurred a possible risk of arrest if a criminal chose to change batteries.[53] It is an economic decision, to be sure. Once an offender possesses a customer's data on an ATM or credit card's magnetic stripe, the information must be copied on either a new debit or credit card or a blank gift card.[54] Although a new debit or credit card can be challenging to obtain, a blank gift card is relatively easy to acquire. Retail stores are replete with offers, asking their customers to purchase gift cards to be used at their stores.[55] Many gift cards hang from hooks that are placed conveniently next to checkout counters. It is a small matter for a criminal, or an accomplice, to procure several of these cards while the criminal is purchasing goods at the store. The designs on ATM or credit cards periodically change, making it difficult for an attendant at a cash register to scrutinize a given card.[56] Most people just take the card out of their wallet, swipe the card, and then put the card back into their wallet. In some instances, merchants require customers to show an ID before making an debit or credit card purchase.[57] Of course, most ATM or credit cards have a person's name and expiration date embossed on the front of the card. By using an embossing machine and possessing the name of the actual cardholder, a criminal can efficiently emboss that data onto a card.[58] debit and credit cards also have a three-digit security code printed typically in italics on the back of a card.[59] A criminal can print any number on the back of a fake

[31] Id.
[32] Id.
[33] Id.
[34] Id.
[35] Id.
[36] Id.
[37] Lorenzo Franceschi-Bicchierai, *Researchers Turn Square Reader into Credit Card Skimmer in 10 Minutes*, MOTHERBOARD, (2015), https://motherboard.vice.com/en_us/article/researchers-turn-square-reader-into-credit-card-skimmer-in-under-10-minutes.
[38] Dave Delozier, *Universal Gas Pump Keys Increase Vulnerability To Skimming*, CHANNEL3000.COM, (2016), http://www.channel3000.com/news/money/universal-gas-pump-keys-increase-vulnerability-to-skimming_20161114071752538/155796089.
[39] Bureau of Weights and Measures, *Skimming Devices in Retail Motor Fuel Dispensers*, NEW YORK DEPARTMENT AGRICULTURE AND MARKETS, (2015), http://www.mass.gov/ocabr/docs/dos/skimmer-presentation.pdf.
[40] Brian Krebs, *Stealthy, Razor Thin ATM Insert Skimmers*, KREBS ON SECURITY, (2012), http://krebsonsecurity.com/2014/08/stealthy-razor-thin-atm-insert-skimmers/.
[41] Id.
[42] Id.
[43] Jenna Deangelis, *Card Skimmer Found At West Hartford Gas Station*, FOX61, (2017), http://fox61.com/2017/02/02/card-skimmer-found-at-west-hartford-gas-station/.
[44] Brian Krebs, *ATM Skimmers, Part II*, KREBS ON SECURITY, (2010), http://krebsonsecurity.com/2010/02/atm-skimmers-part-ii/.
[45] *Id.*
[46] Id.
[47] Kim Zetter, PIN Crackers Nab Holy Grail of Bank Card Security, WIRED MAGAZINE, (2009), https://www.wired.com/2009/04/pins/.
[48] Brian Krebs, Sophisticated ATM Skimmer Transmits Stolen Data Via Text Message, KREBS ON SECURITY, (2010), http://krebsonsecurity.com/2010/06/sophisticated-atm-skimmer-transmits-stolen-data-via-text-message/.
[49] Id.
[50] Id.
[51] Ryan Hughes, Investigator: Criminals Using Elaborate Skimmer Devices to Steal Credit Card Info, WFLA.COM FLORIDA, (2016), http://wfla.com/2016/07/19/investigator-criminals-using-elaborate-skimmer-devices-to-steal-credit-card-info/.
[52] Id.
[53] Id.
[54] How Do Credit Cards Get Cloned?, CREDITNET, (2017), http://www.creditnet.com/Library/Credit_Card_FAQ/How_do_credit_cards_get_cloned.ccfaq_019.php.
[55] Ray Martin, Attention shoppers: Avoid this Gift Card Scam, CBS MONEY WATCH, (2012), http://www.cbsnews.com/news/attention-shoppers-avoid-this-gift-card-scam/.
[56] Id.
[57] Sonya Stinson, Can Retailers Ask for ID with Your Credit Card?, CREDITCARDS.COM, (2013), http://www.creditcards.com/credit-card-news/can-retailers-ask-id-with-credit_card-1282.php.
[58] Paul Muschick, ID Thief Mass-Produced Credit Cards on Embossing Machine, THE MORNING CALL, (2016), http://www.mcall.com/news/local/watchdog/mc-counterfeit-credit-cards-identity-theft-watchdog-20160625-column.html.
[59] Teresa Bitler, How to Find Your Credit Card Security Code, CREDITCARDS.COM, (2017), http://www.creditcards.com/credit-card-news/credit-card-verification-numbers-security-code-1282.php.

ATM or credit card because the number is never used when making a retail purchase at a physical store. If a criminal decodes the information on a magnetic strip, he or she may have access to the real security code.[60] The criminal should print the actual security code on the back of the fake debit or credit card because it is the correct code for the real card. If a criminal prints the existing three-digit security code on the back of the fake card, then the card can be used for electronic transaction purposes, purchasing commodities from Amazon.com, e-Bay.com, and other e-commerce websites.[61] With the advent of chipped ATMs and credit cards, banks are attempting to address illegal skimming without interfering with the convenience of using debit or credit cards.[62] In the United States, banks employ a chip-and-signature technology, whereas, in Europe, a chip-and-pin technology is used.[63] Rather than install a skimmer at a retail store or a gas station, criminals who favor chip-skimming may recruit restaurant staff to skim a chip using a hand-held skimmer that attaches to cell phones and is commonly advertised on television commercial these days.[64] After a meal, a customer typically gives a waiter or waitress his or her ATM or credit card so that the customer can pay the bill. The waiter or waitress takes the card usually to a computer terminal where the card is swiped for payment. At this time, a waiter or waitress can also swipe the card on a hand-held device, thereby skimming the information contained on the chip.[65] This scenario also holds if a waiter or waitress desires to scan the magnetic strip's information. Most waiters and waitresses make low wages and thus have a considerable incentive to engage in skimming as a means to supplement their income.[66] What is evident is that debit and credit card technology is changing in reaction to the skimming pandemic. It has been suggested that and radio frequency identification (RFID) chip be implanted in human beings.[67] Although this idea may have merit, it suffers from the same problems that ATM and credit cards experience.

A Brief History of Skimming

Skimming is a form of identity theft, where data that is encoded on the magnetic stripe on the back of an debit or credit card is read by the skimming device to be later copied onto a fake ATM or credit card.[68] Identify theft is an illegal activity that is based on the fraudulent use of identifying information about a person.[69] Identity theft has a long and illustrious history. In early American history, identity theft was centered around voter registration fraud and ballot stuffing to ensure that a particular candidate was elected to political office.[70] The repeal of Prohibition by the 21st Amendment made it once again legal to consume alcoholic beverages. From the 1930s to the mid-1980s, the legal drinking age was determined by the states. In 1984, the US Congress passed the National Minimum Drinking Age Act, where the minimum age of 21 was established to purchase and consume alcohol legally.[71] Before this time, young men and women, typically under 21 years old, would travel across state lines to buy alcohol in states where 18 or 19 was the minimum age to buy liquor. Often, a fake ID was employed as an early form of identity theft to facilitate underage drinking.[72] Another common form of identity theft occurred in the 1960s with the influx of illegal immigrants and the Immigration and Nationality Act passage.[73] Before the Act, migrant workers would freely come to the United States during the harvest season, performing various unskilled labor activities, and then return to their native country.[74] In 1986, Congress passed the Immigration Reform and Control Act, whereby all employers were required to fill out for each employee a US Citizenship and Immigration Services form, also known as an I-9 form.[75] This Act prodded illegal immigrants to obtain social security numbers and driver's licenses, which in turn stimulated new identity theft.[76] The first universal credit card was the Diner's Club card, which was invented in 1950.[77] The card was an immediate success, and in 1958, American Express created its universal credit card.[78] In 1958, Bank of America issued its credit card in California, which was licensed in other states in 1966, and renamed VISA in 1976.[79] Also, in 1966, a group of banks joined together, creating the Interbank Card Association, issuing Master Charge, now known as MasterCard.[80] This card required cooperation among American banks, forming what has come to be referred to as an *open-loop* system. In contrast, American Express, Diner's Club, and Discover Card are *closed-loop* systems because only one bank was involved in processing transactions using these credit cards.[81] Not to be outdone, significant retailers, sometimes in affiliation with major banks, started issuing their credit cards. These credit cards were known as *revolving charge cards* because a customer need not pay off the outstanding balance at the end of each month.[82] In the later part of the 20th Century, many credit card holders spent more money than they were able to repay due to the high-interest rates and penalties.[83] This situation was exacerbated in 2008-09 due to the Great Recession, high unemployment, and the volume of defaults and bankruptcies. As early as 1984, banks began issuing Debit Cards, which were similar to credit cards, but where purchases were directly subtracted from an

[60] Kas Thomas, *How to Decrypt Credit Card Data, Part I*, ID TECH, (2016), http://www.idtechproducts.com/blog/entry/how-to-decrypt-credit-card-data-part-i.
[61] Paul Ducklin, *How to Guess Credit Card Security Codes*, NAKED SECURITY, (2016), https://nakedsecurity.sophos.com/2016/12/05/how-to-guess-credit-card-security-codes.
[62] Ellie Zolfagharifard, *Will you be a victim of digital pickpockets? Hacker Reveals How Easy It Is to Steal Credit Card Numbers in Seconds While You Still Have Them in Your Hand*, DAILYMAIL.COM, (2015), http://www.dailymail.co.uk/sciencetech/article-2948212/Will-victim-digital-pickpockets-Hacker-reveals-easy-steal-credit-card-numbers-air-SECONDS.html.
[63] David Roos, *How Chip and PIN Credit Cards Work*, HOW STUFF WORKS, (May 16, 2014), http://money.howstuffworks.com/personal-finance/debt-management/chip-and-pin-credit-cards.htm.
[64] Lee Mathews, *Square's Mobile Payment System Has Been Hacked. Twice.*, GEEK.COM, (August 05, 2011), https://www.geek.com/chips/mobile-payment-processor-square-hacked-twice-1410009/.
[65] Id.
[66] Phaedra Cook, *How to Protect Credit Card Data in Restaurants and Bars*, HOUSTON PRESS, (February 01, 2016), http://www.houstonpress.com/restaurants/how-to-protect-credit-card-data-in-restaurants-and-bars-8109648.
[67] *What the Heck Is This Computer Chip Doing in My Credit Card*, HEARTLAND BLOG, (February 22, 2015), https://www.heartlandpaymentsystems.com/blog/2015/02/22/what-the-heck-is-this-computer-chip-doing-in-my-credit-card.
[68] Skimming, supra, note 3
[69] Id.
[70] Loraine C. Minnite, An Analysis of Voter Fraud in the United States, DEMOS, (2003), http://www.demos.org/sites/default/files/publications/Analysis.pdf.
[71] NATIONAL MINIMUM AGE DRINKING AGE ACT, 23 U.S.C. § 158 (1984).
[72] Alex Koroknay-Palicz, Legislative Analysis of the National Minimum Age Drinking Act, NATIONAL YOUTH RIGHTS ASSOCIATION, (n.d.), http://www.youthrights.org/research/library/legislative-analysis-of-the-national-minimum-drinking-age-act/.
[73] IMMIGRATION AND NATIONALITY ACT, PUB. L. 89–236, (June 30, 1965). The Act is also known as the Hart–Celler Act.
[74] Tanya Basu, How the Past 50 Years of Immigration Changed America, TIME, (September 27, 2015), http://time.com/4050914/1965-immigration-act-pew/.
[75] Id.
[76] Id.
[77] The Story Behind the Card, DINER'S CLUB INTERNATIONAL, (n.d.), https://www.dinersclubus.com/home/about/dinersclub/story.
[78] Introducing the Modern Credit Card, BANK OF AMERICA, (n.d.), http://about.bankofamerica.com/en-us/our-story/birth-of-modern-credit-card.html#fbid=sCvG2Xpc3iU.
[79] Id.
[80] Jose Vazquez, The History of MasterCard, GO BANKING RATES, (January 08, 2009), https://www.gobankingrates.com/credit-cards/the-history-mastercard/.
[81] Closed Loop Card, INVESTOPEDIA, (n.d.), http://www.investopedia.com/terms/c/closed-loop-card.asp-0?ad=dirN&qo=investopediaSiteSearch&qsrc=0&o=40186.
[82] Revolving Account, INVESTOPEDIA, (n.d.), http://www.investopedia.com/terms/r/revolving-account.asp.
[83] Ryan Kilpatrick, U.S. Credit Card Debt Tops $1 Trillion for the First Time Since the Recession, FORTUNE MAGAZINE, (April 07, 2017), http://fortune.com/2017/04/10/credit-card-debt-trillion-dollars/.

individual's bank account.[84] With the public intimately at ease with using credit cards, debit cards became popular with the proliferation of Automatic Teller Machines, also known as ATMs.[85] Thus, as America progressed into a cashless society, criminals began to appear to exploit the vulnerabilities in the omnipresent ATM and credit card environment. In December of 2002, CBS News correspondent, Jerry Bowen, reported that thieves siphoned off $1,800 from her bank account using a skimmer device.[86] Before this CBS News report, it was believed that skimmers, tiny devices that could siphon off a person's name, account number, along with other financial information encoded on debit and credit cards, were either a fairy tale or an urban legend.[87] It turned out that Bowen and 80 other customers at a San Mateo gas station were scammed out of approximately $200,000.[88] On October 30, 1998, President Clinton signed into law the Identity Theft and Assumption Deterrence Act.[89] The Act made it illegal to steal an individual's identification information to commit an unlawful act.[90] Congress amended the Act several times, the last time being March 9, 2006.[91] The Act made it illegal for an individual to knowingly (1) transfer identify information to a document (i.e., ATM or credit card); (2) possess a false or fake document with the intent to use unlawfully or transfer said information; (3) commit a financial transaction using said information; and (4) aid or abet and another person with the intent to commit a fraudulent transaction. The penalties that are specified in the Act range from moderate to severe. An individual may be levied a fine and imprisonment ranging from one to 30 years, depending on the offense's severity.[92] As of 2011, 31 states and Puerto Rico had enacted criminal penalties for employing credit card skimming devices,[93] ranging from a misdemeanor with a $1,000 penalty in California and West Virginia[94] to severe felonies with no more than ten years in prison with at most a $20,000 fine in Louisiana.[95] The federal and state penalties are significant. It is entirely possible that an offender could be convicted of skimming in a federal court, serving his or her sentence, only to be tried and convicted for the same offense in the state court where the crime took place. The reason is that the federal and state governments are separate sovereigns, where being convicted of identity theft by the federal government is no guarantee that a state would abdicate its desire to extract its pound of flesh. As a variation of identity theft, skimming is regarded by federal and state law as a serious crime. Given the law's harshness, the issue is whether federal and state governments are enforcing the laws as currently written. As we shall see, the answer depends upon the amount of money stolen and over what period.

What Is the Issue with Skimming?

Because the use of skimmers involves identity theft, it is a federal felony to steal ATM or credit card information from individuals. The issue is whether skimmers' use is sufficiently severe to warrant additional and substantial police action by local, state of federal law enforcement and further legal penalties than what already exists.

HOW IS SOCIETY AFFECTED BY SKIMMING

Skimming affects the (1) the structural characteristics of the legal and societal systems in the United States; (2) the psychosocial qualities of both the criminal and the victim; (3) the technical procedures of how skimming is accomplished; (4) the ways and means that the legal system, banking system, and society as a whole mitigates the problems caused by skimming; and (5) how the goals and objectives of law enforcement, the legal system, the banking system, and the society have changed because of the ever-present threat of skimming.[96]

Structural Characteristics

As skimming has become a common way for a criminal to steal and exploit another person's identity, citizens have had to modify their behavior, and institutions have had to create methods and procedures to catch these criminals, if not at least to record their unlawful conduct. Customers are becoming increasingly wary of using card swiping machines at retail outlets. ATM card and credit card companies are inserting chips into their cards, thereby making it increasingly challenging to skim a cardholder's data. With chips in debit and credit cards, a given transaction's length of time has increased dramatically.[97] Gone are the days when a customer merely takes out their card, quickly swiping the card through the magnetic card reader. This action happens almost instantly.[98] However, when a customer inserts his or her card so that the machine can read the chip's contents, the transaction time can be substantial, particularly with the card reader having difficulty reading the chip's content for one reason or another.[99] When people in line are waiting to pay for their goods, the extra transaction time can become significant. Customers may decide to delay their purchase, opting for a more convenient and less hectic time to purchase their desired goods.[100] The cumulative additional time can act as an economic deterrent to consumption, thereby having a recessionary impact.[101]

Psychosocial Qualities

The word *psychosocial* is concerned with what goes on in people's heads and how people behave based on their feelings, beliefs, and thoughts.[102] In today's world, where the daily news abounds with reports on terrorist activities, most people live in a state of fear.[103] Individuals are afraid that when they step out of the confines and relative safety of their homes, they can be physically assaulted by criminals, have their identity stolen in the most innocent of circumstances, or even be killed for no apparent reason in a violent terrorist attack.[104] The reasonable conclusion is that fear for one's safety is the order of the day. In my case, I have decided to never swipe my ATM card in a card reader at a gas pump. I now go inside

[84] M. Lambert, *The History of Debit Cards*, BRIGHT HUB, (July 06, 2011), http://www.brighthub.com/money/personal-finance/articles/42073.aspx.
[85] *Automated Teller Machine – ATM*, INVESTOPEDIA, (n.d.), http://www.investopedia.com/terms/a/atm.asp?lgl=myfinance-layout-no-ads.
[86] Sue Chan, *Is Your Credit Card Being Skimmed?*, CBS EVENING NEWS, (December 06, 2002), http://www.cbsnews.com/news/is-your-credit-card-being-skimmed/.
[87] Id.
[88] Id.
[89] IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT, (1998), 18 U.S.C. §1028.
[90] Id.
[91] IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT,18 U.S.C. §1028 AS AMENDED BY PUBLIC LAW 105-318 (2006).
[92] Id.
[93] Heather Morton, *Identity Theft*, NATIONAL CONFERENCE OF STATE LEGISLATION, (n.d.), http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx.
[94] Id.
[95] Id.
[96] DON HARVEY & DONALD R. BROWN, AN EXPERIENTIAL APPROACH TO ORGANIZATIONAL DEVELOPMENT (Prentice-Hall (6th ed. 2001).
[97] Jemal R. Brinson, *Why Do New Chip Cards Take So Long?*, CHICAGO TRIBUNE, (April 11, 2016), http://www.chicagotribune.com/business/ct-how-chip-cards-work-htmlstory.html.
[98] Id.
[99] Ian Kar, *The Chip Card Transition in the US Has Been a Disaster*, QUARTZ, (2016 Jul 29), https://qz.com/717876/the-chip-card-transition-in-the-us-has-been-a-disaster/.
[100] Id.
[101] Id.
[102] Don Harvey & Donald R. Brown, *supra*, note 96.
[103] Andrew McGill, *Americans Are More Worried About Terrorism Than They Were After 9/11*, THE ATLANTIC, (September 08, 2016), https://www.theatlantic.com/politics/archive/2016/09/american-terrorism-fears-september-11/499004/.
[104] Id.

the store and then pay for the gas. I check the machine to see if any overlays are readily discernable. If I feel that the card reader is operating to my satisfaction, I use my debit card to purchase the gas. In many gas stations, cameras have not yet been installed. When I am forced to swipe my card, I experience a certain level of fear and trepidation. I recall how I felt when my banker told me that I had been skimmed. I wonder, if only for a second, whether I will be skimmed again, only this time it will be for a lot more money. When I insert my ATM card into the slot where the chip in my card is read, I experience a relative sense of ease. Although I remember how I felt when I learned that I was skimmed, I have the confidence that it will never happen again, even though my intellect tells me that I am experiencing a misguided sense of security. I remember the adage: "Once burnt, twice shy." I try to ignore my feelings and focus on the fact that the legal and banking systems are working, at least hopefully for now.

Technological Procedures

Card issuers have put RFID chips on their cards to reduce the incidence of skimming. These companies have worked closely with card reader manufacturers to ensure that a consistent technical security level is present when customers electronically purchase goods and services.[105] Because there is a certain amount of variety in how the new card readers work, the reading of the magnetic stripe on the back of an debit or credit card has been relegated to a backup system's status.[106] In other words, if, for some unknown reason, if the machine cannot read the chip in the ATM or credit card, a customer can still swipe the card so that the information contained on the magnetic strip can be successfully read. Furthermore, some customers are technological laggards who rebel against using a chip when making a transaction.[107] They feel comfortable swiping their debit or credit cards. After all, habit is a dominant human characteristic, usually dying rather slowly, despite the fact that chip usage is probably technologically safer than card swiping.[108] There are probably two reasons why card issuers migrated from magnetic strips to computer chips. A magnetic strip can be easily read and easily reprogrammed. All a criminal has to do is read the current data on the card into the memory of a device, decrypt the data, and then write the data onto a fake card. This is a straightforward procedure. Because most ATM and credit cards are less than a sixteenth of an inch in thickness, the chip in the card is relatively small. The chips are known as RFID chips and can only transmit information when a specific radio frequency is passed near them.[109] The data is stored in the Europay, MasterCard, and Visa (EMV) format chip.[110] The chip itself does not possess an independent power source, so the only time when information can be transmitted is when the chip is exposed to a particular radiofrequency.[111] Once the information is read, the machine discontinues emitting the specific radio frequency, and the data on the chip is relatively secure.[112] The difference between these chips and the RFID chips that have been inserted in pets for decades is that the former is several orders of magnitude smaller than the latter and can hold much more data.[113]

Mitigation Issues

The existence of a chip inside an ATM or credit card indicates that card issuers and merchants understand that a significant number of individuals are being skimmed and that the problem needs to be mitigated effectively.[114] According to the United States Secret Service, $1 billion is lost every year from ATM skimming.[115] In 2014, it was estimated that 31.8 million Americans were victims of identity theft, and the reason was that the United States has been slow to implement the EMV standard.[116] Although there may be some delay, if an individual knows their rights, the person will likely get their money back after being skimmed.[117] Someone has to pay the bill. According to the Fair Credit Billing Act, the maximum liability for the unauthorized use of a personal debit or credit card is $50.[118] The money usually comes from a consumer who typically pays the insurance premiums for skimming protection in the form of higher monthly fees.[119] Because we live in a free enterprise economic system that idolizes maximizing profits or equivalently minimizing costs, greed is the prime motivator for converting from magnetic strips to RFID chips, even though the United States has lagged behind Europe in its implementation.[120]

Societal Goals and Objectives

The goal of criminals who steal ATM and credit card information is to profit financially from the activity without experiencing incarceration. Customers want to go about their daily business without being interrupted or inconvenienced by having their debit or credit card information stolen. Customers do not want to experience the loss of their card use, and they do not want to be financially inconvenienced. In other words, customers want their financial institution to reimburse them for any money that was stolen. Finally, the banks' goals and objectives, savings and loans, and credit unions that issue ATM or credit cards maximize their profits or equivalently minimize their costs. Thus, in the current economic climate, skimming allows (1) criminals to profit financially instead of being caught, prosecuted, and incarcerated; (2) customers to break even though they may experience some degree of inconvenience in the form of a slight increase in fees, and (3) financial institutions to experience a modicum of loss while passing on any lost income to their customers in the form of higher fees.

THE LEGAL AND SOCIETAL OPTIONS AVAILABLE

There are a variety of legal and societal options. The first alternative is commonly known as the *do-nothing alternative*.[121] With this alternative, whatever law enforcement procedures are in place or whatever laws currently exist are sufficient to solve or mitigate the

[105] Don Harvey & Donald R. Brown, *supra*, note 96.
[106] Komando Staff, *Why There's a Chip in Your New Credit and Debit Cards*, KIM KOMANDO, (2017 Apr 17), http://www.komando.com/tips/328980/why-theres-a-chip-in-your-new-credit-and-debit-cards/all.
[107] GEOFFREY A. MOORE, CROSSING THE CHASM (Harper Business Book rev. ed. 2002).
[108] Komando Staff, *supra*, note 106.
[109] Id.
[110] Id.
[111] Id.
[112] Id.
[113] Jane McGrath, *How Pet Microchipping Works*, HOW STUFF WORKS, (April 21, 2008), http://science.howstuffworks.com/innovation/everyday-innovations/pet-microchip.htm.
[114] How to Identify and Mitigate Skimming Attacks at the Point of Sale, VISA BUSINESS NEWS, (June 09, 2016), https://www.vantiv.com/content/dam/vantiv/merchants-partners/Visa_Business_News_How_to_Identify_and_Mitigate_Skimming_Attacks_at_the_POS__1_.pdf.
[115] BWest Byte: How Much Money Is Lost to ATM Skimming Every Year? (Bloomberg television broadcast May 9, 2017), https://www.bloomberg.com/news/videos/b/993b6ce6-4b6a-4359-b01f-237d0345a394.
[116] Tamara E. Holmes, Credit Card Fraud and ID Theft Statistics, CREDITCARDS.COM, (September 15, 2015), http://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.
[117] Bob Sullivan, Know Your Rights on Bank Account Fraud, NBCNEWS.COM, (August 12, 2008), http://www.nbcnews.com/id/8915217/ns/technology_and_science-security/t/know-your-rights-bank-account-fraud/#.WTddTaBvHh0.
[118] Lost or Stolen Credit, ATM, and Debit Cards, FEDERAL TRADE COMMISSION, (August, 2012), https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.
[119] Lindsay Konsko, Who Pays When Merchants Are Victims of Credit Card Fraud?, NERDWALLET.COM, (June 03, 2014), https://www.nerdwallet.com/blog/credit-cards/merchants-victims-credit-card-fraud/.
[120] Tamara E. Holmes, supra, note 116.
[121] Don Harvey & Donald R. Brown, supra, note 96.

problem. There is nothing to be done. The system will take care of itself. The second alternative is to hold all of the business that in the chain of liability responsible. If debit or credit card information is illegally obtained at a gasoline station, a convenience store, or a retail outlet, whether big or small, then that business should be held at least partially responsible for the identity theft.[122] The theft probably occurred on business premises, and it is questionable what effort the organization made to prevent the crime.[123] The business could blame its low-level employees for not being diligent. However, if an employee is acting in his or her employer's interests, the company is responsible for the employee's actions under the theory of respondent superior. The firm would have to show that an employee intentionally acted in furtherance of their interests and not the company's interests. This is a difficult hurdle to jump over, mainly because when an employee is processing a sales transaction, they are acting in their employer's interests.[124] The third alternative is what could be called the *criminal enforcement alternative*. In other words, law enforcement should be actively and aggressively be involved in finding, arresting, and prosecuting identity thieves.[125] The problem with this option is that the amount of money stolen due to ATM or credit card identity theft is relatively tiny. For example, a Department of Justice study found that the combined average loss due to identity theft was $1,343 per victim and is usually not a violent crime.[126] The theft can be the product of a ring of criminals engaging in a lucrative illegal enterprise. It can be caused by petty criminals attempting to profit unlawfully from the unsuspecting public.[127] The fourth alternative is to educate consumers about skimming and what they can do to mitigate the problem. On its face, this seems like a viable solution, but when one looks closer, it becomes apparent that the alternative is riddled with issues that inhibit its implementation.[128] First, consumers are primarily interested in conducting their own business without worrying about the threat of identity theft.[129] Customers are usually not interested in collecting detailed information about the nature of skimming. All they are interested in is getting their money back and then going about their business.[130] A consumer could take active steps to prevent identity theft in the future. A customer could decide to monitor his or her bank statements, credit reports, as well as shredding sensitive documents, etc.[131] The idea is that the more aware one is regarding the dangers of identity theft, the fewer opportunities there will be for criminals to steal one's financial information.[132] In my opinion, this is an idea that makes good sense. However, there are problems with this alternative. For example, when an individual decides to use his or her debit or credit card less frequently than they previously did, financial institutions lose.[133] The fees that merchants pay the card issuers every time a customer uses their card would decrease. This means less revenue for financial institutions and thus lower profits.[134] The consumer may believe that they are risk-averse by using only cash, but the economy experiences a decline due to the paradox of thrift.[135] According to the paradox of thrift, when consumers save rather than consume, the economy suffers.[136] When consumers pay for goods using cash, financial institutions do not profit from the transaction. The merchant is not paying the financial institution a percentage of the cost of the good.[137] Although this revenue loss is slight for individual consumers, in 2014, a Department of Justice study observed that identity theft losses in the United States amounted to about $15.4 billion annually.[138]

Should Society Discourage Skimming?

After considering the four options listed above, it is apparent that the average amount of damages is insufficient to warrant economic or legal action beyond what is currently being done.[139] By progressively converting ATM and credit cards into cards that use RFID chips employing the EMV standard, financial institutions are taking practical steps to limit their losses and their customers' losses.[140] The only alternative that would have a more significant effect on restricting identity theft would be to inject each person with their RFID chip. However, such an action would spawn a possible revolt among the American people.[141] The citizenry would fear an unprecedented invasion of their privacy. It would play into the hands of conspiracy theorists who would exploit the already present fear of oppression in the population.[142]

The Consequences of Combating Skimming

What are the implications of seemingly doing nothing? It is a misnomer to say that nothing should be done about the problem. The alternative suggests that the legal system, and society as a whole, should take somewhat of a laissez-faire approach to the issue, where market forces are responsible for solving the problem, rather than insisting that the government address the matter.[143] The chosen response acknowledges that the market with current administration oversight is implementing a viable solution. The RFID chip using the EMV standard is the answer that the market has embraced, and it

[122] Deanne Katz, *Customer ID Theft: Are Businesses Liable?*, FINDLAW: FREE ENTERPRISE BLOG, (January 30, 2013), http://blogs.findlaw.com/free_enterprise/2013/01/customer-id-theft-are-businesses-liable.html.

[123] *Beware of "Red Flags": What Must Your Business Do to Protect Customers from Identity Theft?*, WARD AND SMITH, P.A., (2017), http://www.wardandsmith.com/articles/what-must-your-business-do-to-protect-customers-from-identity-theft.

[124] *Meyer v. Holley*, 537 U.S. 80 (2003), https://supreme.justia.com/cases/federal/us/537/280/#tab-opinion-1961167. Here, the Court held that the Fair Housing Act imposed liability without fault on the employer based on traditional agency principles.

[125] *Flores-Figueroa v. United States*, 129 S.Ct. 1886 (2009), https://scholar.google.com/scholar_case?case=16662764610021735982&hl=en&as_sdt=6&as_vis=1&oi=scholarr. Here, the Court held that the Government had to show that the defendant knew that the means of identification at issue belonged to another person. The judgment of the Court of Appeals was reversed, and the case was remanded for further proceedings.

[126] Cody Gredler, *The Real Cost of Identity Theft*, CSIDENTITY, (September 09, 2016), https://www.csid.com/2016/09/real-cost-identity-theft/.

[127] Nicole Hong, *More Street Gangs Turn to Financial Crimes*, WALL STREET JOURNAL, (March 07, 2016), https://www.wsj.com/articles/more-street-gangs-turn-to-financial-crimes-1457379074.

[128] *When Bad Things Happen to Your Good Name*, FEDERAL TRADE COMMISSION, (November 2003), http://www.iwar.org.uk/ecoespionage/resources/id-theft/idtheft.pdf.

[129] Ann Noder, *Identity Theft Survey Results: Consumers Need More Education and Help*, THE NEW YORK TIMES, (May 15, 2017), http://markets.on.nytimes.com/research/stocks/news/press_release.asp?docTag=201705150600PR_NEWS_USPRX____LA89973&feedID=600&press_symbol=3744729.

[130] Id.

[131] Identity Theft & Credit Card Fraud – How to Protect Yourself, WALL STREET JOURNAL, (n.d.), http://guides.wsj.com/personal-finance/credit/how-to-protect-yourself-from-identity-theft/.

[132] Id.

[133] Melissa Lamberna, How Do Credit Card Companies Make Money?, NERDWALLET, (April 06, 2017), https://www.nerdwallet.com/blog/credit-cards/credit-card-companies-money/.

[134] Id.

[135] PAUL KRUGMAN & ROBIN WELLS, ECONOMICS (Worth Publishers 2nd ed. 2009).

[136] Id.

[137] Melissa Lamberna, supra, note 133.

[138] Cody Gredler, supra, note 126.

[139] Taylor Tepper, Here's Why Your Credit Card Now Has a Chip and Why You Should Care, TIME.COM, (September 28, 2015), http://time.com/money/4040808/credit-card-chip-fraud-emv/.

[140] Id.

[141] Jon Austin, Mark of the Beast: Secret plan to 'implant us all with ID chips by 2017', EXPRESS, (August 25, 2016), http://www.express.co.uk/news/weird/703856/MARK-OF-THE-BEAST-Secret-plan-to-implant-us-all-with-ID-chips-by-2017.

[142] Id.

[143] Identity Theft, UNITED STATES DEPARTMENT OF JUSTICE, (n.d.), https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

seems to be effective.[144] Current data indicates that skimming has declined 52 percent at EMV-enabled stores.[145] Although there is always the possibility that criminals will outsmart financial institutions, and come up with even better strategies to defraud the naïve public, it remains to be seen if criminals will be able to circumvent the security employed by debit and credit cards containing RFID chips using the EMV standard.[146] Criminals may go in a different direction, say e-commerce fraud.[147] Only time and experience will answer this question.

CONCLUSION

The conclusion selected may be dissatisfying to individuals who want the government to solve the identity theft problem. However, whether the government can solve the skimming problem without violating fundamental rights such as the right to privacy has yet to be seen. On an individual basis, the damages resulting from skimming appear to be relatively unsubstantial. The recovery mechanisms available to both consumers and financial institutions seem to be working reasonably well. The market has decided to verify a person's identity using RFID chips using the EMV standard rather than the information encoded on the magnetic strips that are located on the back of debit and credit cards. Short of a radical technology change, this seems like an excellent solution to me.

[144] Debit Technical Working Group, *U.S. Debit EMV Technical Proposal*, EMV MIGRATION FORUM, (April 2014), http://www.emv-connection.com/wp-content/uploads/2014/04/US_Debit_Technical_Solution_V1.2-Final.pdf .
[145] Jennifer Bellemare, *Have EMV Chip Cards Helped Decrease Identity Theft?*, IDENTITY FORCE, (February 17, 2017), https://www.identityforce.com/blog/emv-chip-cards-decrease-identity-theft.
[146] Id.
[147] Kim Zetter, *That Big Security Fix for Credit Cards Won't Stop Fraud*, WIRED, (September 30, 2015), https://www.wired.com/2015/09/big-security-fix-credit-cards-wont-stop-fraud.

****