The Bill Blackwood
Law Enforcement Management Institute of Texas

Credit Card Fraud and Fuel Pump Skimming

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Jason Burton

Tyler Police Department
Tyler, Texas
June 2021

ABSTRACT

Credit card fraud and fuel pump skimming affected 16 million Americans in 2018, impacting the U.S economy with 16.8 billion dollars in losses (ABA Banking Journal, 2018). Fuel pump skimmers are placed inside the fuel pump, giving consumers no clue as to its presence. When a credit or debit card is swiped through the card reader, the device captures and stores all the details stored in the card's magnetic strip. The strip contains the credit card number, expiration date, and the credit card holder's full name. Thieves use the stolen data to make fraudulent charges, either online or with a counterfeit credit card.

Law enforcement should investigate these types of crimes aggressively, using the most up-to-date technology available. In order to effectively combat these issues, departments need to make these crimes a priority by allocating appropriate personnel and providing up-to-date training. Investigators need to network with banking employees as well as federal agencies, such as the Secret Service and FBI. By providing training, not only to other law enforcement agencies, but to the owners of fuel sites themselves, law enforcement can have a large impact on the cyber safety of our citizens.

TABLE OF CONTENTS

INTRODUCTION

Credit card fraud is a national epidemic that affected 16.7 million Americans in 2018, which was a record high that followed a record of the previous year (Insurance Information Institute, n.d.). Criminals are engaging in complex schemes that cost victims 16.8 billion dollars in 2018 (ABA Banking Journal, 2018). The Consumer Sentinel Network (CSN), which is maintained by the Federal Trade Commission, tracks fraud cases that are filed with federal, state, and local law enforcement agencies. Credit card fraud was the most reported incident according to CSN, with the median amount paid by consumers being $429 (ABA Banking Journal, 2018).

The CSN went on to say that cybercrimes continue to grow as criminals find new technology and practices. McAfee and the Center for Strategic and International Studies (CSIS) estimate that the likely annual cost to the global economy from these types of crimes is $445 billion dollars (ABA Banking Journal, 2018). Credit card fraud affects several different parties, such as credit card holders, banks, and merchants. Of these three, the actual cardholder bears the least of the burden. According to the Fair Credit Billing Act, if a consumer's credit card is stolen, or used fraudulently, the most they can be liable for is $50 (The Balance, 2020). Debit cards are a different story. Debit card holders can be held accountable for none or all the charges depending on when the fraud is reported to the bank. Because cardholders have very limited liability under federal law, banks and merchants bear most of the burden, which they, in turn, pass on to consumers with higher prices and fees.

In recent years, criminals have moved to fuel pump skimming to gain consumers' credit/debit card information. Fuel pump skimmers are placed inside the fuel pump and

collect the consumer's card number and PIN. One fuel pump skimmer can collect hundreds of consumers' information daily. Thieves are then able to collect this data and either sell it on the dark web, or clone cards themselves, which they then use to purchase gift cards from legitimate businesses. Sometimes, consumers have no idea they have been victimized until they receive their statement and find fraudulent charges. By the time this occurs, it is usually too late for law enforcement to do much about it.

In 2017, the top 3 states for fraud were California, Florida, and Texas (Insurance Information Institute, n.d.). In Texas, Houston seems to be a staging point for gangs committing these types of crimes. According to Sgt. J. Nowitz of the Harris County Sheriff's Office, "Houston is one of the hotbeds for fuel pump skimming cases in the country" (Gill, 2018, para. 6). Tyler Police Investigators also report that Cuban organized criminal enterprises have moved into the Houston area from Florida and are responsible for a large portion of fuel pump skimming in Texas. Investigators have teamed with the U.S. Secret Service to try to combat these groups. It is clearly evident, that credit card fraud and fuel pump skimming are not going away anytime soon. Law enforcement agencies should aggressively investigate gas pump skimming cases using the most up-to-date technology and training available.

POSITION

Credit card fraud and fuel pump skimming affected 16.7 million Americans in 2018 (Insurance Information Institute, n.d.). The ease in which thieves can retrieve personal information digitally makes every consumer a target. Credit card skimming is a type of credit card theft where crooks use a small device to steal credit card information in an otherwise legitimate credit or debit card transaction. When a consumer swipes

their credit or debit card through a card reader, if a skimmer has been installed, the skimming device captures and stores all the details stored in the card's magnetic strip. The strip contains the credit card number, zip code, expiration date and the credit card holder's full name. Thieves are then able to use the stolen data to clone fraudulent credit cards in the victim's name. They then use these fraudulent cards to purchase legitimate gift cards or make purchases online (Irby, 2018). Fuel pump skimmers are placed inside the actual fuel pump, giving victims no clue as to its presence. One skimming device can store hundreds of card numbers daily. One of the more prevalent questions asked is how criminals get the skimming devices inside the fuel pumps. Unfortunately, the keys for most pumps are identical and readily available on the internet. Once inside the pump, thieves are able to attach the skimmer in a matter of seconds. Thieves normally target smaller convenience stores that have no video surveillance, poor video surveillance, and old gas pumps. Criminals seem to prefer placing their devices on the outermost pumps, away from the view of the store clerk.

In the past, the skimming devices themselves had to be removed from the fuel pumps in order to extract the information. In early 2018, law enforcement began seeing a shift to using Bluetooth technology. It is now possible for suspects to simply drive into the area of the skimmer and receive the data electronically, either on a laptop computer or smart phone. Another way criminals are retrieving this data is through the use of SMS messaging. When a card number is collected, the information is immediately sent to the thief via a text message. This makes it harder for law enforcement to identify where a skimmer might be placed and identify who might be retrieving the information.

Suspects then take this information and either sell it to other criminal enterprises or transfer it to blank credit cards, which they then use fraudulently.

There are several different ways thieves are able to use these fraudulent cards. One of the most prevalent is to use the fraudulent cards to purchase gift cards from legitimate businesses. Thieves in Tyler, Texas have been caught purchasing several thousands of dollars in gift cards from one store. Yet, another scam involves the use of large trucks with external fuel tanks. Criminals gather the credit card data from the skimmer and then use it to purchase large amounts of diesel fuel. The thieves take this fuel to legitimate businesses where they sell it and collect the profit.

Victims of credit card fraud and skimming are subject to many different issues. When a victim's credit card information is stolen and fraudulently used to purchase goods, the Fair Credit Billing Act limits the amount of liability they can incur to $50 (The Balance, 2020). Victims whose debit card information is stolen face a whole different challenge. When debit card information is stolen and used fraudulently, consumers only have 48 hours to notify the financial institution (The Balance, 2020). When the 48-hour deadline is met, victims may only be held liable for up to $50 of the loss (The Balance, 2020). If the fraud is reported after the 48-hour period, but before 60 days of the loss, consumers can be held liable for up to $500 (The Balance, 2020). In cases where the fraud is not reported until after the 60 day deadline, victims can be held liable for the entire amount of the loss (Bacon, 2016).

Taking into consideration that consumers can only be held accountable for up to $50 in credit card fraud, the largest portion of the loss gets pushed back to the bank that issued the credit/debit cards. Looking at the progression of loss, the first institution to

lose money is the bank. Since the cash to make the purchases comes from banks, they must reimburse the cardholder for their loss. Banks then rely on law enforcement to investigate the offense in order to hold the criminal responsible. Under most circumstances, the individuals or groups that committed the fraud are not going to pay unless convicted in a court of law, and legal cases could take months or years to complete. In an attempt to recoup some of their losses, banks will often point to poor security or technological issues with the merchants that allowed them to be compromised in the first place (Oldshue, 2014).

Merchants carry a different, but significant, burden when it comes to credit card fraud. When merchants sell their products to criminals using fraudulent credit cards, they are out of product with a difficult road to getting it back. Banks often look to the merchant for reimbursements. Since the bank is immediately responsible for reimbursing the cash to the card holder, they often point to security and technology issues with the merchant that allowed the fraud to take place. If there is a certain amount of fraud that occurs at a given store, payment processors could move to terminate the merchant's account. Further, the store could be placed on a blacklist, meaning it may be very difficult to find another payment processing firm. Most of the larger businesses and corporations can absorb these types of losses, but they can be crippling for the small business owners (Oldshue, 2014). In the end, the losses incurred by the banks and merchants usually end up being pushed back on all consumers by way of increased banking fees and higher prices in stores.

COUNTER ARGUMENTS

The ease of installing skimmers and the overall lack of proactive policing has created a wide-open market for criminals to exploit the system. Sad to say, police rarely investigate credit card fraud. Most of the time, this is not because they don't want to; rather, because they simply can't. This is due to many factors. For starters, credit card fraud is often not reported. Since most consumers are protected by federal law against any major liability, most just cancel their cards at the first sign of fraud. Also, the nature of credit card fraud as a non-violent crime makes it a less pressing matter for the police, compared to, say, murder. With most police departments having limited resources to investigate crimes, fraud cases are often left on the sidelines unless they have personnel to spare or it involves a substantial amount of money (Stone, 2018). Unfortunately, in the United States, departments are struggling to find enough qualified applicants for the jobs available. According to the Bureau of Justice Statistics, in 2016 there were about 700,000 full-time, sworn officers working in this country (Law Enforcement Bureau of Statistics, 2016). That number of officers is a drop of 23,000 officers since 2013 (Inskeep & Kaste, 2018). Law enforcement is being asked to do more with less. Due to these issues, the investigation of credit card fraud often takes a back seat to other, more high-profile, cases. Investigators must manage an already heavy case load, giving them very little time to invest in these very intricate, hard to investigate, cases. According to Investigators with the Tyler Police Department, one investigation can lead to many different suspects, in many different states. Networking and having proper assistance from the different federal agencies can help agencies without appropriate resources.

With the exception of a few cutting-edge offices like the Tyler Police Department and Smith County District Attorney, the vast majority of American police agencies and offices have received very little training in how to investigate and prosecute credit card skimming cases. Investigators with the Tyler Police Department have taken the lead on investigating credit/debit card fraud in Texas. They have partnered with the Secret Service and are aggressively investigating these crimes. At a Tyler City Council meeting, Ed Broussard, the Tyler city manager, said that the Tyler Police Department noticed a skimming issue and worked with business owners to reduce their use, prompting the Attorney General's Office to take note (Campbell, 2018). During an interview, City Manager Ed Broussard said, "We're quite proud of the fact that Tyler is leading the state in this and helping to educate and teach other departments around the state on how to be able to reduce those risks to Texans and others that are visiting the state," (Campbell, 2018, para. 5).

In 2018, detectives with the Tyler Police Department, assisted by the U.S. Secret Service, recovered 96 skimmers in Smith County and another 41 in Tyler. Their investigations led to the arrest of 30 suspects from Houston, Austin, Dallas-Fort Worth and Florida (Campbell, 2018). Most of these suspects were charged with engaging in organized criminal activity and received prison sentences ranging from 15 to 30 years, which sends a very powerful message (Campbell, 2018).

The cost associated with investigating credit card fraud, debit card fraud, and fuel pump skimming can be high. According to the now-defunct National Petroleum News' Market Facts, there are approximately 153,000 fueling stations in the U.S (Munk, 2017). Only a small portion of these fueling sites are owned by large oil corporations. What

this means is that the bulk of stations are owned by independent operators who do not possess the deep pockets of these larger oil companies.

One-way credit card companies are trying to improve security is through the use of Europay, MasterCard and Visa's (EMV) anti-counterfeiting security technology. This poses a significant problem for the independent owner, in that the "average cost to upgrade one single pump to EMV technology runs anywhere from 6,000 and 10,000 dollars" (Munk, 2017, para. 12). In 2020, Mastercard and Visa will require all fuel pump owners to install EMV technology in order to shield themselves from liability. As one can see, operators are not legally required to upgrade their pumps, but, if they do not, they can be held liable for a portion of the fraud. To many, this will turn into a simple business decision. Many operators may ask themselves how much it will cost to upgrade their pumps and question the type of liability they could incur if they do not. There are several different programs that will assist smaller, often unbranded, stations with no money up front. Gas Pos, a startup company out of Birmingham, Alabama has designed an EMV upgrade module that plugs into the existing pumps and communicates an encrypted signal back to the store, meeting all the guidelines of the credit card company. According to Gas Pos CEO, Joshua Smith, this can save customers $30,000 dollars in capital expenses (Cision, 2018).

Credit card fraud and fuel pump skimming affected 16.7 million people in 2018 alone, and the total reported cost of the fraud reached $16.8 billion dollars (Insurance Information Institute, n.d.). According to the FBI, there were 4,251 bank robberies in the United States in 2018 (Averill, 2018). The average amount stolen in these bank robberies is $3400, making the total economic impact a little over $14 million dollars

(Averill, 2018). As one can see, credit card fraud losses are over $16 billion greater than bank robberies. With law enforcement facing these types of criminal enterprises, there is no possible way they cannot dedicate the appropriate amount of trained personnel to combat the issue.

RECOMMENDATION

Credit card fraud and Fuel Pump Skimming cost Americans $16.8 billion dollars in 2018; therefore, law enforcement should aggressively investigate these cases, (Insurance Information Institute, n.d.). The ease in which citizens can fall victim to these crimes confirms the fact that law enforcement needs to do everything in its power to protect them. Fuel pump skimmers are very easily placed in gas pumps all over the United States, and, unknowingly, steal 16 million peoples' personal credit card and debit card information (Irby, 2018). Thieves are then able to take this information and sell it on the dark web or use it to clone counterfeit credit cards. When this credit card information is stolen and used fraudulently, according to the Fair Credit Billing Act, consumers are only liable for up to $50 of the loss (The Balance, 2020). Debit card users find themselves in a whole different situation. Depending on the time frame in which they report the fraud, they can be held liable anywhere from $50 to the entire amount of the loss (The Balance, 2020). The rest of the liability is felt by the banks and merchants. Banks are forced to raise their fees to offset the losses. Merchants can face the same fate as the banks, in that they lose merchandise, time, and money.

The ease of installing credit card and debit card skimmers, coupled with less than proactive policing by law enforcement, has created a wide-open market for criminal gangs to profit from. Law enforcement fails to properly investigate these crimes due to

manpower and the complexity of the investigation. Departments with these issues would benefit from joining multi jurisdiction task forces as well as seeking assistance from federal agencies like the Secret Service and the FBI. In early 2019, HB 2945 was passed by the legislature, creating the first Financial Crimes Fusion Center. This center will be housed in Tyler, Texas and offer free training to law enforcement professionals all across Texas. Officers from the Tyler Police Department will be tasked with collecting and analyzing data from all across the state. This data will be available to any law enforcement agency seeking assistance (House Bill 2945, 2019).

Costs associated with investigating and preventing credit card fraud and fuel pump skimming can be high. Credit card companies like Master Card and Visa will begin requiring fuel pump owners to install EMV technology inside their fuel pumps beginning in 2020, in order to shield the fuel station of liability. The cost associated with adding this technology to existing fuel pumps ranges anywhere from $6,000 to $10,000 (Munk, 2017, para. 12). The majority of fuel centers in the U.S are independently owned, and most owners cannot afford this outlay of capital. Gas Pos, a company located in Alabama has developed an EMV module that can plug into the existing gas pump and communicate an encrypted signal back inside the store (Cision, 2018). The company is offering this technology to fuel station owners at no up-front cost to them (Cision, 2018). Fuel center owners can also take advantage of several other secure ways of paying, like Google Pay.

As one can see, there are several ways that fuel station owners and consumers can protect themselves from becoming victims of these crimes. Consumers need to be very aware of their credit and debit card accounts and report any suspicious activity

immediately. Station owners need to be vigilant of suspicious activity at their pumps and embrace the many different payment options that do not require the use of a credit card. Furthermore, all agencies need to consult with their District Attorney's offices to discuss options for prosecuting these cases. The victories won by the Tyler Police Department along with the Smith County District Attorney prove that these criminals can be caught and prosecuted very effectively. With the implementation of the Financial Crimes Fusion Center, a wide range of training will be available to assist in the investigation of credit card skimming. Agencies must seek out this training and use it to the best of their abilities.

REFERENCES

ABA Banking Journal. (2018, February 12). *Report: Total number of fraud victims tops 16 million.* Retrieved from https://bankingjournal.aba.com/2018/02/report-total-number-of-fraud-victims-tops-16-million/

Averill, V. (2018, October 31). Are there 2400 bank robberies per year in the US? [Answer 1]. Answer posted to https://www.quora.com/Are-there-2400-bank-robberies-per-year-in-the-US

Bacon, N. (2016). When banks can can refuse to refund fraudulent debit card charges. M*agnify Money.* Retrieved January 21, 2019, from https://www.magnifymoney.com/blog/identity-theft-protection/banks-refuse-refund-fraudulent-charges21625321/

Campbell, L. (2018, June 27). Tyler police department discusses gas pump skimmers at Attorney General's office in Austin. *Tyler Morning Telegraph*. Retrieved from https://tylerpaper.com/news/local/tyler-police-department-discusses-gas-pump-skimmers-at-attorney-general/article_8292bdf8-7a52-11e8-bc77-f7db74e913ad.html

Cision. (2018, October 3). *Gas pos brings relief to nationwide gas pump cost crisis.* Retrieved from https://www.prnewswire.com/news-releases/gas-pos-brings-relief-to-nationwide-gas-pump-cost-crisis-300723578.html

Gill, J. (2018, November 14). A 'hotbed': Prevalence of gas pump skimming in Houston area underscored by lack of data. *Houston Chronicle*. Retrieved from https://www.houstonchronicle.com/

House Bill 2945. (2019). Enforcing Prohibition on Payment Card Skimmers at Gas Stations. Retrieved from: https://hro.house.texas.gov/pdf/ba86R/HB2945.PDF

Inskeep, S. (Interviewer) & Kaste, M. (Interviewee). (2018, December 11). *Shortage Of Officers Fuels Police Recruiting Crisis* [Interview transcript and audio file]. Retrieved from National Public Radio website: https://www.npr.org/2018/12/11/675505052/shortage-of-officers-fuels-police-recruiting-crisis

Insurance Information Institute. (n.d.). Facts + Statistics:Identity Theft and Cybercrime. Retrieved November 9, 2020, from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

Irby, L. (2018). How credit card skimming works. *The Balance.* Retrieved January 17, 2019, from https://www.thebalance.com/how-credit-card-skimming-works-960773

Law Enforcement Bureau of Justice Statistics. (2016). 2016, from https://www.bjs.gov/content/pub/pdf/nsleed.pdf

Munk, C. (2017, September 18). Why many gas stations don't want EMV - and what they're doing instead. *Payments Source.* Retrieved from https://www.paymentssource.com/news/why-many-gas-stations-dont-want-emv-and-what-theyre-doing-instead

Oldshue, L. (2014, June 11). Who pays for fraudulant credit card transactions? *Low Cards.* Retrieved from https://www.lowcards.com/pays-fraudulent-credit-card-transactions-24850

Stone, J. (2018, August 6). How do the police investigate credit card fraud? [Answer 3]. Answer posted to https://www.quora.com/How-do-the-police-investigate-credit-card-fraud

The Balance, (2020, July 29). Who is Responsible for Stolen Credit Card Charges? Answer posted to https://www.thebalance.com/your-liability-for-stolen-credit-card-charges-961073