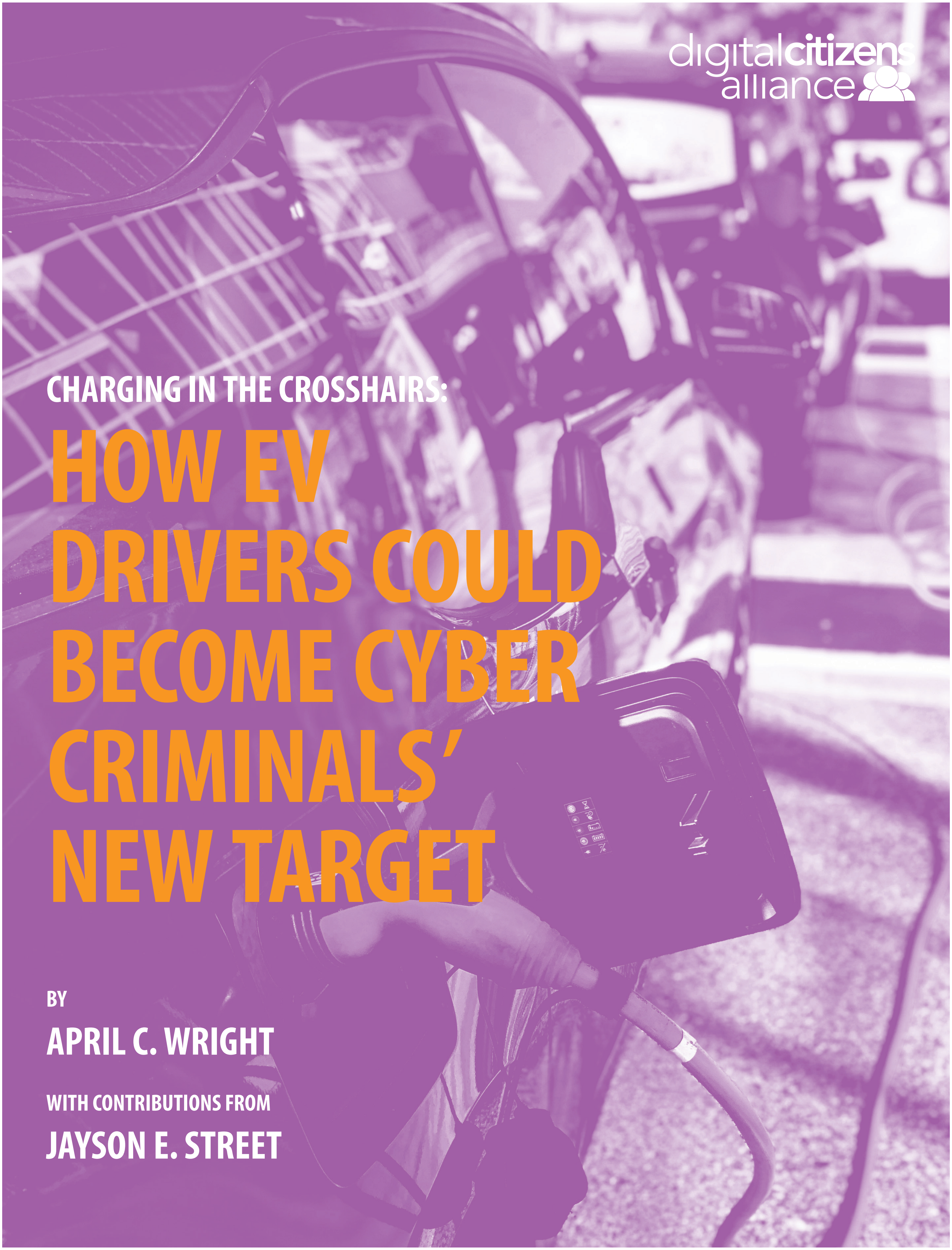


digitalcitizens alliance

CHARGING IN THE CROSSHAIRS:

HOW EV DRIVERS COULD BECOME CYBER CRIMINALS' NEW TARGET

BY

APRIL C. WRIGHT

WITH CONTRIBUTIONS FROM

JAYSON E. STREET

CHARGING IN THE CROSSHAIRS:

HOW EV DRIVERS COULD BECOME CYBER CRIMINALS' NEW TARGET

BY

APRIL C. WRIGHT

WITH CONTRIBUTIONS FROM

JAYSON E. STREET

EXECUTIVE SUMMARY

Electric vehicle (EV) drivers could soon become targets for cyber criminals if proposals that mandate the installation of credit card readers at public charging stations are approved.

Payments made at EV charging stations currently rely on “contactless” methods using the latest in digital technologies – including mobile payments over smartphones and RFID cards.

Over the last year, the Digital Citizens Alliance has focused on the security of devices for consumers because as we create a more connected world, the risk of exploitation also increases. This extends to how consumers pay for services. The proposed mandate of credit card readers at EV charging stations that include technologies such as Magnetic Stripe Reader (MSR) would be a step backward from a consumer security standpoint because the readers are a frequent target of criminal enterprises and individual hackers.

Compounding the problem, many EV charging stations are unmonitored, unattended, and located in remote areas along highways and in parking garages. This provides an opportunity for criminals to install malicious devices without being detected. This could make EV drivers an easy target for cyber criminals, exposing them to credit card fraud and identity theft.

THE CHALLENGE: PROTECTING EV DRIVERS FROM FRAUD

With a growing number of EVs on the road and dozens of new models hitting showrooms soon, the safety and security of EV charging stations should be paramount.

Yet, mandating credit card readers would expose drivers to new security risks and put them in the crosshairs of cyber criminals who use ‘skimmers’ and ‘shimmers’ to commit fraud.

Skimmers and shimmers – small, easy-to-obtain devices engineered to steal credit card data – are a rampant problem today at gas stations and other point-of-sale (POS) terminals. Cyber criminals can plant them on otherwise legitimate credit card readers in a matter of seconds, and they are difficult for consumers to detect.

Fraud related to these devices has become such a widespread threat that the U.S. Secret Service has launched a nationwide crackdown with regular alerts to law enforcement, service stations and drivers. In November 2018, the Secret Service announced it had removed nearly 200 devices at gas stations across 16 states, and this is only a small percentage of the total devices actively exploiting cards.

Stolen credit card data can be used for fraudulent purchases or sold on the Dark Web. The costs can be staggering, and retailers are hit hard by fraudulent purchases that often cannot be recovered. Fraud rings can use the stolen data to commit additional crimes including identity theft.

MANDATING CREDIT CARD READERS WOULD EXPOSE DRIVERS TO NEW SECURITY RISKS AND PUT THEM IN THE CROSSHAIRS OF CYBER CRIMINALS WHO USE ‘SKIMMERS’ AND ‘SHIMMERS’ TO COMMIT FRAUD

At a time when credit card fraud and identify theft cost Americans $16 billion annually, this problem will worsen if new credit card reader mandates are approved for EV charging stations.

CURRENT PROPOSALS

Across the nation, there are currently several credit card reader proposals under consideration.

- In California, the California Air Resources Board (CARB) would mandate all operators of public EV charging stations in the state to install credit card readers on their stations.
- NESCAUM – an association of eight Northeast and Mid-Atlantic states – is considering whether to issue a recommendation for all member states to establish requirements for credit card readers at publicly funded EV charging stations.
- In Nevada, the Governor’s Office of Energy (GOE) issued a mandate requiring credit card readers at all Direct Current Fast Charge (DCFC) projects that receive funding through the state’s “dieselgate” settlement with Volkswagen.
- In Vermont, the state agencies overseeing Volkswagen’s settlement spending issued a mandate that all DCFC stations that receive funding have credit card readers installed.

- In Arizona, the Corporation Commission is considering best practices for stations deployed by utility investments, which may include mandating payment options such as credit card readers.

While these proposals may be well-intentioned, they could expose drivers to new security risks while providing cyber criminals with easy access to attractive targets.

A common perception is that EV drivers have above-average incomes, so it is hard to imagine a better way to gift cyber criminals with attractive targets.

A BETTER ALTERNATIVE

Rather than mandate credit card readers be made available to users, EV charging stations and other point-of-sale (POS) terminals should continue to feature secure payment methods, such as mobile solutions, and legislators should engage with the security community to better understand fraud risks associated with credit card readers.
The stakes have never been higher.

This paper examines the strengths and weaknesses of various payment options from a security perspective in light of these proposals; describes the practices of cyber criminals; and makes recommendations for how to maintain security in this industry poised for growth.

OVERVIEW

At a time when there are dozens of models of electric vehicles (EVs) on the road and dozens more in development, a raft of new proposals about how payment is made for charging sessions are threatening the security of EV drivers.

WHILE THESE PROPOSALS MAY BE WELL-INTENTIONED, THEY COULD EXPOSE DRIVERS TO NEW SECURITY RISKS WHILE PROVIDING CYBER CRIMINALS WITH EASY ACCESS TO ATTRACTIVE TARGETS.

These proposals are being considered at a moment when the payment card industry (PCI) is struggling with credit card fraud. Even as security mechanisms have become more difficult to hack, fraud has continued to increase.

While credit card fraud impacts virtually all merchant sectors, there are targets for fraud that are of noteworthy concern. The “unattended” payment terminal space (i.e. no cashier taking payment) has become a prime focus for criminals. In particular, gas stations have suffered from widespread and repeated attacks. Payment terminals embedded in gas pumps are often monitored during business hours, but are unattended and thus, offer significant opportunity with which to be tampered.

EV chargers take this a step further. They’re often deployed in environments that are not only “unattended,” but are “unmonitored,” meaning that there is no cashier and there is no one on site actively observing the station. Some are deployed in remote areas vulnerable to tampering and vandalism.

HARMFUL PROPOSALS ON THE TABLE

Unfortunately for consumers, proposals are currently being put forward in several U.S. states and other countries to impose new rules and mandates on EV chargers. The proposals would mandate that EV charging stations be fitted to accept physical credit cards.

These proposals would effectively reverse the industry's careful considerations regarding EV charger payment options.

In one of the first proposals, the California Air Resources Board (CARB) has proposed a rule that would require owners and operators of EV charging stations to replace their existing infrastructure with stations that include credit card Magnetic Stripe Readers (MSRs) and Europay, Mastercard, and Visa (EMV) Chip readers. Such a rule would introduce a higher risk of fraud to EV charging station consumers and operators.

Similar proposals across the country include:

- NESCAUM – an association of eight Northeast and Mid-Atlantic states – is considering whether to issue a recommendation for all member states to establish requirements for credit card readers at publicly funded EV charging stations.
- In Nevada, the Governor's Office of Energy (GOE) issued a mandate requiring credit card readers at all Direct Current Fast Charge (DCFC) projects that receive funding through the state's "dieselgate" settlement with Volkswagen.
- In Vermont, the state agencies overseeing Volkswagen's settlement spending issued a mandate that all DCFC stations that receive funding have credit card readers installed.
- In Arizona, the Corporation Commission is considering best practices for stations deployed by utility investments, which may include mandating payment options such as credit card readers.

THESE PROPOSALS WOULD EFFECTIVELY REVERSE THE INDUSTRY'S CAREFUL CONSIDERATIONS REGARDING EV CHARGER PAYMENT OPTIONS.

WHY THESE PROPOSALS THREATEN CONSUMERS' SECURITY

Credit card fraud is a crime of opportunity, perpetrated by individual criminals and highly sophisticated international fraud rings. If it is easier and more lucrative to commit fraud in one place than another, criminals will direct their efforts to areas where opportunity is maximized.

Credit card theft is so lucrative that it has been a target of organized crime for many years, particularly at gas station pumps. Theft rings and regional fraud schemes are so prevalent that the U.S. Secret Service launched a nationwide initiative – known as Operation Deep Impact – to find and remove credit card theft devices installed on fueling station pumps. In

[1] https://www.brumellgroup.com/news/the-fraud-triangle-theory/

November 2018, the agency announced it removed nearly 200 devices at gas stations across 16 states. This is representative of only a small percentage of the total devices actively exploiting cards.

Given the substantial risks, it is paramount that there be a heightened level of security for EV charging stations.

Today, by encouraging drivers to use contactless payments, EV stations are already deterring credit card fraud.

However, if proposed mandates requiring EV charging stations to accept MSR and EMV Chip cards are approved, EV charging stations will become high-value targets for criminals. This is particularly an issue given the widespread perception that EV drivers have above-average incomes.

MSRS, EMV CHIP AND THE LINGERING PROBLEM OF CREDIT CARD FRAUD

Magnetic Stripe Readers and EMV Chip readers are, by far, the most popular means of non-cash payment in the world. The tens of millions of payment card readers that exist today provide the capability for merchants to accept payment worldwide. The deployment of such devices has been massively successful innovation.

MSRs have been around since the beginning of the 20th century and were first used on credit cards in the early 1970s[2]. Credit card issuers encode information on the magnetic stripe on the card using a varying magnetic field. When a magstripe credit card is passed through a reader, a magnetic reader head outputs a voltage signal that is modulated by the magnetic information on the stripe (based on the current that is induced in a coil of wire within the magnetic head). This varying voltage can be considered audio, and the action is referred to as a "swipe." [3]

One of the issues with MSR is that the magnetic data on the credit card stripe is static, which is why credit cards eventually became a popular target for illegal activity. Criminals utilize cheap and easy-to-obtain tools that can be ordered on the public Internet to commit their crimes.

Over time, security vulnerabilities associated with magstripe technology and MSRs led to the introduction of the EMV ("Europay, Mastercard, and Visa") Chip reader, which has since become a global standard. EMV Chip credit cards are more secure than their MSR predecessor and include the ability to create a unique transaction code used only once for a particular payment.

In the event that data is stolen, the temporary transaction code is not usable for any other transactions. EMV Chips have made payment theft more difficult, particularly in regions where EMV Chip readers are exclusively used.

However, criminals are as motivated as they are skilled, and they have found a way to exploit the highly secure EMV Chip.

Even as the migration to EMV Chip cards and readers continues, the ongoing use of the legacy MSR technology creates a problem for the EMV Chip, and represents a major dilemma for the payment card industry.

[2] https://tedium.co/2015/06/09/credit-card-history/

[3] https://www.blackhat.com/docs/us-15/materials/us-15-Mellen-Mobile-Point-Of-Scam-Attacking-The-Square-Reader-wp.pdf

In North America, the payment card industry has been trying to make MSR obsolete and mandate EMV Chip use since 2011.

An original deadline of October 2015 mandating merchants switch from MSR to EMV Chip based transactions has come and gone. While the number of merchants moving to EMV Chip has dramatically increased, there is no definitive timeline for the full retirement or elimination of MSRs. The time and cost needed to retire tens of millions of terminals deployed worldwide and replace them with EMV Chip readers is an expensive endeavor that will take years, and the next deadline for full EMV migration, October 2020, will likely also come and go.

Some sectors, including those most vulnerable to credit card attack, will not be fully converted to EMV by the next deadline. In fact, many gas stations will be lagging well behind that timeline. As long as MSR remains active, fraud will continue to be a painful problem for the payment card industry, merchants, and consumers.

HOW DOES CREDIT CARD FRAUD TAKE PLACE?

Credit card fraud rings range in size and scope, and their impact can be significant. In January 2019, three people were arrested having racked up $3 million in purchases and possessing 700 stolen accounts.[4] In a 2017 case, 18 hackers were alleged to have stolen over $200 million, possibly the largest organized credit card fraud ring in U.S. history[5] at the time.

The victims are not just the credit card companies or the consumers. Merchants are the hardest hit by fraudulent purchases, with potentially massive losses that often can never be recovered.

Compounding the problem, credit card data obtained on the Dark Web can be combined with other personal data obtained from any of the multitude of database breaches that have occurred in recent years (e.g., Equifax, IRS, OPM, eBay, Yahoo, Cambridge Analytica/Facebook, USPS, Uber, Ancestry.com, Marriott, Hilton, CVS, et al.[6]). The relatively simple act of combining data from these breaches can create more complete “identities” that could contain health data, tax data, SSN, purchase habits, family, employment, location, and more in addition to a valid card.

Identity information makes a card more valuable on the Dark Web because a complete profile of an individual can easily lead to identity theft, which is immeasurably worse for the consumer than credit card fraud alone.[7] Further, if a card was obtained from a certain chain retailer, then additional purchases from that retailer are less likely to be flagged as fraudulent. This also increases the value of a stolen card.

Identity theft is a $16 billion industry affecting more than 16 million Americans annually.[8] It can lead to account takeovers[9] and additional information breaches. If a compiled identity leads to an email account takeover, it could enable password resets, address changes, and other pervasive activities affecting the target person.

[4] https://westfaironline.com/110316/three-arrested-in-new-rochelle-accused-in-3m-stolen-credit-card-ring/

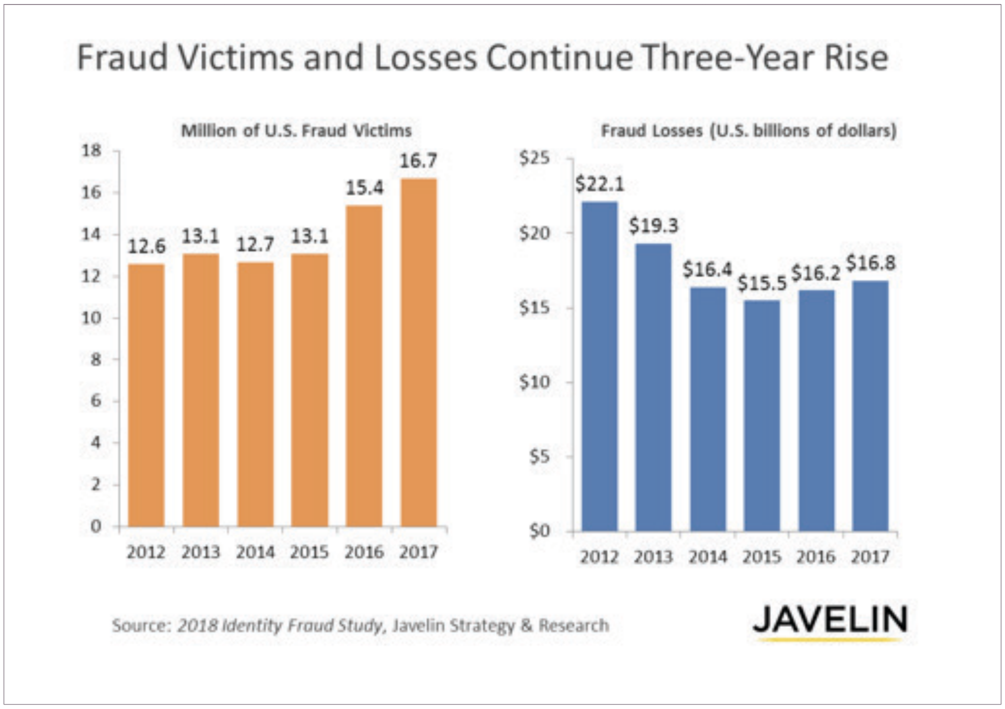
[5] https://www.verifi.com/press-releases-and-announcements/special-report-feds-bust-200-million-credit-card-fraud-ring-2/

[6] https://en.wikipedia.org/wiki/List_of_data_breaches

[7] https://abcnews.go.com/Business/credit-card-stolen/story?id=25633648

[8] https://www.lifelock.com/learn-identity-theft-resources-how-common-is-identity-theft.html

[9] https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity



Source: *2018 Identity Fraud Study*, Javelin Strategy & Research

While it is relatively simple for the average person to obtain an illegal credit card data theft device, it is the level of organization and logistics that make theft rings so dangerous. Criminal enterprises employ people to install and collect theft devices, working across multiple states, using increasingly stealthy technology which they research, develop, and produce themselves. With so much money available to be stolen, criminal organizations are investing a little and walking away with a lot.

IF EMV CHIPS ARE SO SECURE AND IF MOST TERMINALS SUPPORT EMV CHIPS, WHY IS FRAUD STILL AN ONGOING PROBLEM?

EMV Chip readers, when used with EMV Chip cards, are a sophisticated and secure means of processing payment. Yet, no payment method is perfect.

While EMV Chip payments are more secure than MSR, in markets where MSR remains in use, fraud associated with both MSR and EMV Chip is a reality.

While there are various forms of credit card theft, the most popular, lucrative, and widespread form of fraud is by the use of hardware devices called skimmers and shimmers.

A “skimmer” is a malicious device that is embedded in the MSR card reader. When a credit or debit card is swiped through the terminal’s MSR, the skimmer device captures and stores all the details stored in the card’s magnetic stripe before it can be encrypted by the terminal.

In addition to the traditional MSR skimmer, a new device called a “shimmer” has emerged. A shimmer is similar to a skimmer in that it is a malicious device embedded in the payment terminal, however, while still targeting the Magnetic Strip of the card, it is implemented into the EMV chip reader instead of the MSR. [10]

Skimmers and shimmers are hidden inside the card reader and are often completely undetectable by the merchant or consumer. These devices capture, record, and often transmit sensitive card holder data.

While the EMV Chip security is robust, a shimmer can capture MSR related information from the EMV Chip reader which can then be used in subsequent fraudulent MSR transactions. EMV Chip data is difficult to obtain, but the magnetic stripe is still capable of being read if it exists on the card being inserted into the machine. The ongoing use of MSR has perpetuated this vulnerability, which has made shimmers the new hacking tool of choice for cybercriminals in a world that increasingly only accepts EMV Chip payments.

The sophistication and availability of skimmer and shimmer devices has increased in recent years.

The world's top secure payment terminal providers have witnessed precision molded plastic replicas of their payment terminals used to mask the existence of a skimmer or a shimmer.

New technologies exist that attempt to detect and prevent some skimming and shimming devices, but at additional cost to the merchant. And unfortunately, as detection gets better, so too does the criminals' circumvention of detection. Protections implemented by merchants over time become only partially useful and then eventually obsolete.

It is a cat-and-mouse game whereby the terminal providers implement a deterrent and the criminal enterprises' technology adjusts with a countermeasure. Such sophisticated attacks exist on all continents, making payment card related theft a global problem.

REAL-WORLD CREDIT CARD THREATS

Wedge Skimming

- This attack can occur any time the card is not in the possession of the authorized card holder. This is of most concern in places like restaurants, in areas where the driver cannot pump their own gas (like New Jersey), and at other retailers where the POS system is hidden from view.
- One common type of skimming occurs when a salesperson or waitstaff takes the consumer's physical payment card and runs it through a malicious card reader. The malicious reader copies the information contained in the card's magnetic stripe via a skimmer. This can happen when a consumer is paying for something and the merchant's employee walks off with the card to a POS terminal out of sight.
- Once the thief has obtained the card data, they can use or sell it.[11]
- Pay-at-the-table terminals also known as mobile POS (mPOS) have gained acceptance in Europe and elsewhere to help prevent this type of theft. The idea is that if the consumer can see the terminal, the person who is handed the consumer's card is less able to use a separate device to swipe the card and steal its information. However, skimmers can still in theory be installed on mPOS terminals and used covertly.

[10] https://www.consumerreports.org/scams-fraud/thieves-get-craftier-with-skimmers-debit-cards-credit-cards/

[11] https://www.justaskgemalto.com/us/flash-attacks-make-big-money-debit-and-credit-card-scammers/

Skimming and Shimming aka Capture via Hardware[12]

- Skimming is a $2 billion industry [13]
- A malicious card reader can be placed over the face of the existing card reader, reading every card that passes by the skimmer before the card is read by the original mechanism.
- Data is stored or sent to the criminal who installed the device. An overlay device may use a wireless technology like Wi-Fi, Bluetooth, or cellular transmission in order to obtain the captured data remotely.[14]
- To the user, an overlay device appears to be a normal part of the machine. It is incredibly difficult to recognize a skimmer, unless it is not attached well or is of poor quality. Current advice for users is to "jiggle" parts of the device to see if they are loose. This practice does not have a high adoption or success rate.
- Similarly, number pad and button overlays can be installed to capture information entered into the terminal's button pad, usually information such as ZIP code or PIN. Tiny pinhole cameras were once used for this purpose, but button overlays are one example of a technology improvement developed by criminals to make it easier and more reliable to capture data.

Lack of Encryption Leads to Injection and Sniffing Attacks

- At a 2016 hacker conference, security researchers Nir Valtman and Patrick Watson, from U.S.-based POS and ATM manufacturer NCR demonstrated a stealthier and more effective attack technique that works against most "payment points of interaction," including card readers with PIN pads and gas pump payment terminals.[15]
- The main issue shared by many remote (e.g. fuel pump or ATM) payment devices is that they don't use authentication and encryption when sending data back to the POS payment software, usually located in a main building. This exposes data to man-in-the-middle eavesdropping attacks through use of an external device that taps the connection of the main POS system. This allows an attacker to capture data from all pumps or ATMs, rather than from individual payment input devices. However, many modern implementations do encrypt data as soon as it is read at the individual terminal, which can help prevent this type of attack.
- The researchers demonstrated that criminals can use this attack technique to steal magstripe encoded data in addition to being able to trick cardholders into exposing their PIN code (for debit cards) or CVV2 code.
- It is a requirement for PIN pads to encrypt the PIN when transmitting data to the POS software. However, the demonstration proved it is possible to display malicious prompts on the POS terminal screen, meaning an attacker can ask the user to "please enter the 3-digit CVV2 code on the back of the card" or "please re-enter PIN". When the user enters their data following such prompts, the data is not encrypted and can be captured.[16]

[12] https://krebsonsecurity.com/all-about-skimmers/
[13] https://blog.dieboldnixdorf.com/have-you-asked-yourself-this-question-about-skimming/
[14] https://www.justaskgemalto.com/us/flash-attacks-make-big-money-debit-and-credit-card-scammers/
[15] https://www.blackhat.com/docs/us-16/materials/us-16-Valtman-Breaking-Payment-Points-of-Interaction.pdf
[16] https://www.pcworld.com/article/3103925/security/stealing-payment-card-data-and-pins-from-pos-systems-is-dead-easy.html

- Some PIN pads use a whitelist of words which are allowed to appear on custom screens, but many of these whitelists allow the words “please re-enter”.

- Even if words are whitelisted to restrict content, the whitelist can be bypassed because PIN pad custom forms allow images. Thus, attackers could inject an image with any words, using the same text color and font that normally appears on the screen.

Internal Data Interceptors

- Cheap or improperly installed skimmers or shimmers can sometimes be detected by “jiggling” the components of a fueling payment terminal or ATM. This tactic can uncover loose malicious components.

- In another example of improvements developed by criminals to “one up” detection technology, some devices are now using data-stealing devices that are installed inside the pump to conceal the device.

- A criminal can either use readily available lock picks or use a universal key purchased on the public Internet to access the inside of the terminal.

- The cable connecting the keypad to the display is disconnected, and the malicious capture device is placed between those components. The capture device is out of sight with less risk of exposure and able to obtain all the unencrypted card data.[17]

MSR as Input Device

- Building on work from Samy Kamkar and his MagSpoof techniques, along with integrated “bad barcode” technology from Tencent, Rapid7’s Weston Hecker has demonstrated how to inject operating system (OS) commands into a Windows-based POS system via the MSR:

“Often a magstripe reader [MSR] is configured as a general-purpose device, so you can drop in commands to open a register, open a window, or download malware and install,” said Tod Beardsley, senior security research manager at Rapid7.

- When a payment device is programmable via an electromagnetic field (EMF), an attacker can turn the MSR into a keyboard, running commands on the central terminal OS. “You only need to distract the operator for a couple seconds -- it all happens very quickly,” Beardsley explained. [18]

EASY THEFT USING SKIMMERS AND SHIMMERS

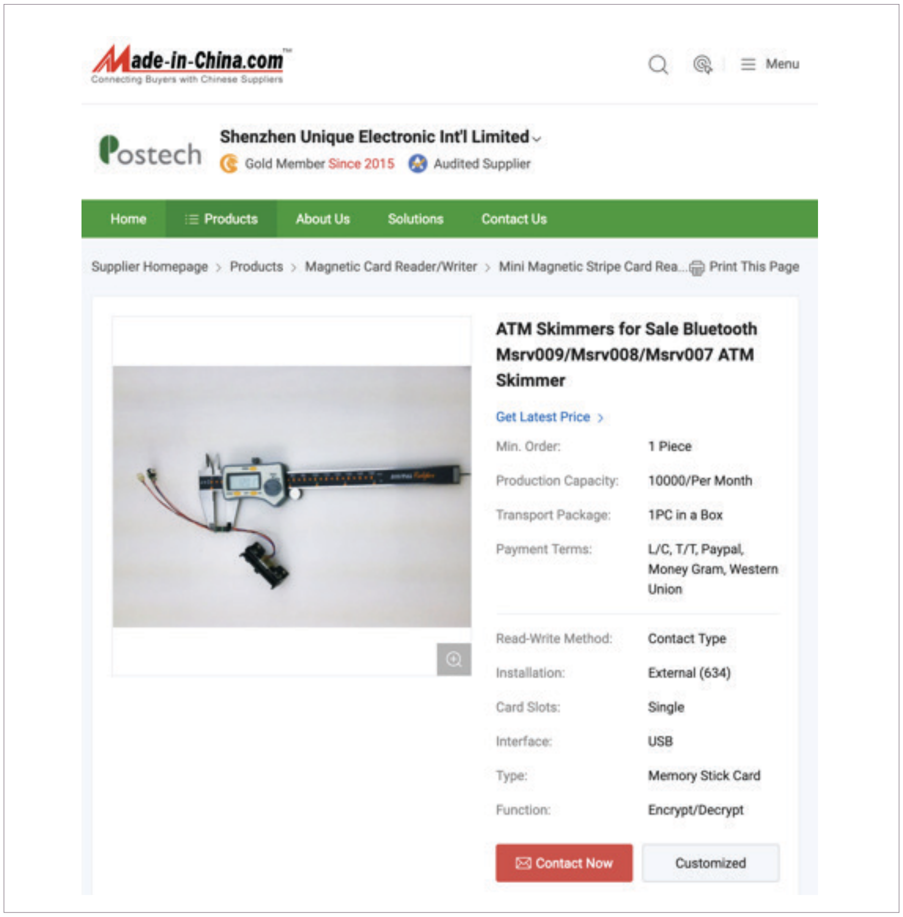
Stealing card information using skimmers at gas pumps and other “unattended” locations (such as ATMs) is not a new problem; it is now an entire industry. Criminals are becoming increasingly sophisticated at hiding the devices and getting around preventative measures that terminal providers, banks, and merchants have deployed.

How easy is it to obtain a skimmer? Anyone can literally just buy one online.[19] Right now. Not on the Dark Web, but on the public Internet.

[17] https://www.justaskgemalto.com/us/flash-attacks-make-big-money-debit-and-credit-card-scammers/

[18] https://www.darkreading.com/vulnerabilities---threats/hotel-pos-and-magstripe-cards-vulnerable-to-attacks-brute-forcing/d/d-id/1326481

[19]


Made-in-China.com
Connecting Buyers with Chinese Suppliers
Menu
Postech
Home
Products
About Us
Solutions
Contact Us
Supplier Homepage › Products › Magnetic Card Reader/Writer › Mini Magnetic Stripe Card Rea...
Print This Page
Get Latest Price ›
Contact Now
Customized

Shenzhen Unique Electronic Int'l Limited

Gold Member Since 2015 Audited Supplier

ATM Skimmers for Sale Bluetooth Msrv009/Msrv008/Msrv007 ATM Skimmer

Min. Order:	1 Piece
Production Capacity:	10000/Per Month
Transport Package:	1PC in a Box
Payment Terms:	L/C, T/T, Paypal, Money Gram, Western Union
Read-Write Method:	Contact Type
Installation:	External (634)
Card Slots:	Single
Interface:	USB
Type:	Memory Stick Card
Function:	Encrypt/Decrypt

Image: An ATM skimmer for sale on the website made-in-china.com

Alternatively, an individual can make a skimmer (or shimmer) using one of the countless instructional videos and articles available on the Internet.[20]

Payment terminals that include MSR and EMV Chip readers represent a risk to the card holders who use them. The degree of risk is directly related to a criminal's ability to access and modify the terminal.

The risk profile for merchants rises significantly when payment terminals are in the "monitored (during business hours), but unattended" sectors, such as gas pumps or ATMs. The risk profile again rises significantly when payment terminals are in the nearly-completely "unmonitored and unattended" sector, such as an EV charging station.

NEW TECHNOLOGY IS AVAILABLE AND ACCESSIBLE

Today, EV manufacturers around the country are ahead of the curve when it comes to protecting against fraud.

EV charging terminals are using a variety of different PCI-approved contactless payment methods while not introducing any MSR

[20] https://cashmoneyskimmer.wordpress.com/2015/04/11/skimmer-building-guide/

vulnerabilities. In the vast majority of transactions, payments at EV charging stations today are made via mobile device (e.g. phone) or via an encrypted RFID card issued to the driver. The strides taken to protect station payments effectively prevent EV charging stations from becoming vulnerable.

Using secure payment apps like Apple Pay or Google Pay protects consumers and merchants better than physical payment cards with less expense to the merchants.

NFC and other contactless payment methods are not without risks (there is no such thing as zero risk), but the risks compared to MSR and EMV Chips are minimal and acceptable due to the benefits NFC provides.

CONCLUSION

If regulatory requirements inadvertently introduce payment security vulnerabilities, the successful rollout of EV chargers would be harmed at a critical juncture in the state of the industry.

Magnetic Stripe Readers and EMV Chip readers are the most common payment methods used today and service a vital means for consumers to have a variety of payment options. However, until the day comes when Magnetic Stripe Readers are discontinued, POS devices that use Magnetic Swipe Readers and EMV Chip readers will continue to be vulnerable to attacks.

The remote, unmonitored, unattended nature of EV charger deployments make them an unacceptable risk to integrate Magnetic Swipe Readers and EMV Chip readers. Simply put, it can be expected that EV chargers would surpass gas pumps as the most inviting target for skimmer and shimmer fraud.

At a time when the EV and EV charging industry continues to grow, imposing integration of MSR and EMV Chip readers into EV chargers would represent a unnecessary risk to all EV drivers.

ABOUT THE AUTHORS

APRIL C. WRIGHT is a cybersecurity expert with more than 25 years of experience educating consumers, organizations and policymakers on security and privacy risks in the digital age and working with them to strengthen their networks and prevent breaches. She speaks at cybersecurity conferences across the globe and has worked with a variety of government agencies, industry associations and businesses.

JAYSON E. STREET is Vice President of Information Security at SphereNY. He is a renowned cybersecurity expert, hired by leading companies and banks to "legally hack" their networks and identify vulnerabilities. He has been featured in National Geographic, FOX Business, Ars Technica, Scientific American and CSO Magazine.

ABOUT DIGITAL CITIZENS ALLIANCE

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders—individuals, government and industry—to make the Web a safer place. Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. **Visit us at digitalcitizensalliance.org**

digitalcitizens alliance