

**Testimony of James Hurst
New York City Department of Consumer Affairs**

**Before the
New York City Council Committee on Consumer Affairs**

**Hearing on
Introduction 1406, regarding Nonbank ATMs**

January 12, 2017

Good morning, my name is James Hurst and I am the Director of Enforcement for the New York City Department of Consumer Affairs (“DCA”). I am joined today by my colleagues, Alba Pico, Mary Cooley, and Casey Adams. I would like to thank the committee for the opportunity to testify on Introduction 1406 (“Intro. 1406”), which would mandate certain security measures and other practices for owners and operators of Automated Teller Machines (“ATMs”) that are not affiliated with banking institutions. DCA shares the Council’s goal of making nonbank ATMs safer and more secure, as well as improving the options available for low income New Yorkers to access their hard earned assets. We look forward to discussing the best way to achieve those goals with the committee.

DCA’s new mission is to protect and enhance the daily economic lives of New Yorkers to create thriving communities. We serve New York City’s consumers, businesses, and working families, enforcing laws and providing services that address the needs of New Yorkers, from their wallets to their workplaces. DCA also operates the Office of Financial Empowerment (“OFE”), the first local government initiative in the country with the mission to educate, empower, and protect New Yorkers and neighborhoods with low incomes, so they can build assets and make the most of their financial resources. OFE conducts research to better understand the issues facing low-income New Yorkers and potential barriers to accessing safe and affordable financial services.

Since they first appeared in 1996, nonbank ATMs have become a common sight in New York City’s corner bodegas, bars, and restaurants. Indeed, many of the types of businesses that host ATMs, like bodegas and gas stations, are already regulated and inspected by DCA. New Yorkers rely on these machines for fast access to their cash and are willing to pay a premium, in the form of “out-of-network” fees, for the service. However the fees associated with this convenience may be more burdensome to lower-income New Yorkers, who also tend to have fewer options for accessing their own money. In a recent study, DCA found that there are currently 360,000 households in New York City who do not have a bank or credit union account.¹ Moreover, there are an additional 780,000 households who are underbanked, meaning they have a bank account but continue to use check cashers, nonbank money orders and prepaid cards.² For many unbanked

¹ Caroline Ratcliffe et al., *Where Are The Unbanked And Underbanked In New York City?* (Urban Institute Sept. 2015), <http://www.urban.org/sites/default/files/alfresco/publication-pdfs/2000430-Where-Are-the-Unbanked-and-Underbanked-in-New-York-City.pdf>.

² *Id.*

New Yorkers, like those with only a prepaid or payroll card, and underbanked New Yorkers, access to cash is extremely important. Many of these New Yorkers must rely on the type of nonbank ATMs this bill addresses.

Most banks allow customers to access their cash at affiliated ATMs without added fees. Under current law, ATMs owned or operated by financial institutions must provide security measures similar to those that would be required for nonbank ATMs by Intro. 1406. For example, bank ATMs must be monitored by security cameras and be adequately lit for consumers during both daytime and nighttime hours. Because there are no similar requirements for nonbank ATMs, unbanked or underbanked consumers face a situation where they may be charged more than a banked individual to use an ATM that is less safe and secure.

In addition, the variety and decentralization of nonbank ATM deployment may make them particularly attractive targets for those who seek to steal personal and banking information using “skimmer” devices. These devices, which vary widely in terms of physical appearance, technical sophistication, and ease of identification, are attached to ATMs in order to harvest sensitive information from unsuspecting consumers. Some of these devices can be identified simply by jiggling the card receiver slot to see if any foreign objects are attached, while others are so well concealed that only an expert would be able to spot them. In a recent report, FICO found that the number of ATMs compromised by criminals rose dramatically in 2015 and that nonbank ATMs were the main targets.³ Intro. 1406 would combat this problem by putting the burden of regularly inspecting ATMs and reporting any suspicious devices on the merchants who host the machines and the distributors who provide them.

DCA supports the intent of Intro. 1406, which is to make nonbank ATMs safer and more secure and protect consumers from skimming and identity theft. At this time, the Law Department is still conducting its review of the bill and all relevant legal issues. We look forward to discussing the specifics of how this legislation would operate, the type of inspection and enforcement actions DCA could take, and how the requirements of Intro. 1406 would interact with existing state and local laws. We also seek to continue the conversation about how DCA and the Council can work together to expand the options available to low income New Yorkers who want to improve their financial health and plan for successful futures. My colleagues and I will be happy to answer any questions you may have.

³ *ATM Compromises in US Jumped Six-Fold in 2015, FICO Reports*, FICO (Apr. 8, 2016), <http://www.fico.com/en/newsroom/atm-compromises-in-us-jumped-six-fold-in-2015-fico-reports-04-08-2016>.



9802-12 Baymeadows Road, #196 | Jacksonville, FL 32256 | O (904) 683-6533 | F (904) 425-6010
EMAIL mail@natmc.org | WEBSITE www.natmc.org

**WRITTEN TESTIMONY OF
THE NATIONAL ATM COUNCIL, INC.
BRUCE WAYNE RENARD, EXECUTIVE DIRECTOR**

JANUARY 12, 2017

Good morning Mr. Chairman and esteemed Committee members, my name is Bruce Wayne Renard and I serve as Executive Director for The National ATM Council, Inc. ("NAC"). NAC is the national trade association dedicated to representing the interests of America's retail ATM industry across the U.S. This includes our many members providing ATM services today throughout the five Boroughs of New York City ("New York", the "City" or "NYC").

NAC sincerely appreciates the opportunity to address the Committee on Int. 1406-2016 (the "Proposed Ordinance"), which would create a new regulatory regime for retail ATMs within New York. **While NAC shares the Chairman's goals of enhancing safety and security for consumers of retail ATMs in New York, NAC respectfully submits that, if enacted in its current form, the Proposed Ordinance would create severe unintended adverse consequences and untenable costs for New York's ATM businesses, merchants, and consumers – without actually improving security for consumers of retail ATM services in the City. NAC would accordingly request that the Proposed Ordinance be tabled in favor of an initiative to increase the criminal penalties and level of enforcement/prosecutorial resources devoted to ensuring ATM safety and security.**

Rather than seeking to legislate a "one size fits all" solution for improved safety at retail ATMs in New York, NAC would respectfully request that the "in the trenches" aspects of ATM security continue to be allowed to be aggressively addressed by ATM industry security professionals, merchants, and law enforcement professionals, working closely together to combat the day-to-day challenges of keeping cash readily and safely available to the public throughout New York.

Most helpful and effective as deterrence to crime against ATMs and those that use or service them is for the Council to:

(1) implement increased criminal penalties and mandatory incarceration sentences for those who commit crimes against ATM terminals and/or those that use or service them (a mandatory five (5) year incarceration sentence for first time offenders committing ATM related crimes would be the most effective deterrent); (2) encourage continued



development of an aggressive and targeted law enforcement protocol to address these specialized crimes; and (3) encourage improved cooperation and communications between industry and law enforcement to develop and implement practical strategies and solutions.

Background and Statement of Interest

NAC's Mission Statement is as follows:

“The National ATM Council, Inc. is a not-for-profit national trade association dedicated to ethically and effectively representing the business interests of ATM Owners, Operators and Suppliers in their efforts to provide safe, secure and convenient delivery of cash to consumers throughout the United States.”

As is readily evident from our charter, ATM safety and security and the ongoing ability to safely delivery cash to consumers across America are key issues for our association and its members. NAC member companies, and the industry as a whole, have every incentive to ensure a safe and secure environment for retail ATMs, and for those that use and service/load them. Safety and security is paramount for ATM service to the public and continued operation of these ATM businesses. Without this, we are out of business – or worse yet, injured or dead. Imposition of regulatory requirements that burden retail ATM providers and merchants, and quickly become technologically outdated, is not the answer. Such a course will not stop criminals, but will instead leave citizens and visitors to NYC without needed cash in the worst of possible situations.

New York ATM Security Initiatives

NAC and our New York membership have been extremely proactive to date when it comes to addressing ATM crimes in the City. We have worked very closely and successfully with the NYPD and the Commissioner's Office to address the scourge of physical crimes against ATMs in NYC, and have made noticeable improvement in reducing these crimes over the past several years. Most recently, our New York ATM provider members have worked closely with local law enforcement to address an uptick in skimming (theft of card/PIN data for fraudulent re-use) activity at NYC retail ATMs.



NAC has also been alerting our members to these recent developments, and we have provided support and tools for our members to address these issues effectively “in the trenches”, along with merchants and law enforcement. (See attached Member Alert example.)

National ATM Security Initiatives

At the national level, NAC has worked diligently to educate and support America’s ATM industry regarding crime prevention and protection for ATM providers and those we serve. Most recently, NAC presented an in-depth ATM Security Academy (“ASA”) program as a key component of its annual conference. The faculty for this program included some of America’s top security professionals and law enforcement representatives, providing a wealth of information and insights on ATM safety and security. NAC is making a video of the program available to all our members and conference attendees, and would be glad to work with the City in making the information available to all ATM providers that operate in New York.

Of particular recent interest and attention by NAC is the increased threat of card skimming at retail ATMs fostered by implementation of the EMV chip card technology effectively mandated by the global card networks. To gauge the scope of the skimming problem, in early 2016 NAC conducted an industry-wide survey regarding the nature and extent of skimming at retail ATMs. (See Attached Survey Summary Results.) The survey of a statistically valid sample of ATM companies across America indicated that more than nine out of ten providers had never experienced even one single skimming incident at their retail ATMs – with more than half of the providers having been in the ATM business for ten years or more. These survey results tracked the anecdotal evidence NAC had received from its members, that most of the card skimming occurs at bank ATMs (those with much higher volumes and most often with no live “attendants”), rather than at retail ATMs (those with far lower transaction volumes – and with live store personnel present).

Notwithstanding these findings, NAC recognized that skimming at retail ATMs could spike with the advent of EMV chip card technology now being implemented in the U.S. To address this concern, last year NAC reached out to Connexus, the technology/standards setting body for the National Association of Convenience Stores (“NACS”), to develop an “anti-skimming guide” for use at convenience stores/bodegas throughout America (the “Guide.”) The Guide (copy attached) explains how best to avoid



skimming crimes and enforces proper protocol to follow if a skimmer is detected. NAC's Guide has since been distributed to thousands of ATM providers and merchants across the U.S., highlighted at NAC's recent trade show, and made available by NAC and NACS to all members and the industry generally on an ongoing basis.

Retail ATMs are Serving an Important Public Interest

It is vitally important that the Committee and the Council understand the role retail ATMs play in ensuring widespread access to cash in NYC. It is equally important to understand that this industry sector is currently facing enormous economic burdens and is simply not able to fund the new regulatory costs or the substantial capital requirements stemming from the Proposed Ordinance. If enacted, the Proposed Ordinance would irreparably harm not only ATM providers and bodega owners across the City, but also seriously harm the many citizens and visitors who rely on these retail ATMs for convenient access to cash and for essential access to EBT funds.

The so called "non-bank" ATMs singled out under the Proposed Ordinance are actually ATMs placed into service pursuant to a contractual arrangement with a "sponsorship bank". Sponsor Banks are chartered financial institutions that extensively investigate all prospective ATM providers, before being allowed to participate in the ATM business and on an ongoing basis once in operation. These sponsored ATMs are provided at locations other than on a bank premises. They are typically provided by small/medium sized entrepreneurial businesses. Importantly, these ATMs serve those areas where there are no bank branches or bank owned/operated ATMs close by. They often serve in the lower economic areas where bank presence is sparse, as well as many public locales such as universities, hospitals, hotels, airports, sports stadiums, and government buildings.

The Proposed Ordinance Will Harm NYC ATM Providers, Merchants and Consumers – Without Improving Safety for Consumers

Please note that each ATM placement is unique to the specific location, in terms of ideal placement, employee and public access, and overall security considerations. The Committee should also note that security "best practices" change continually, depending on the nature/level of local criminal activity and the ongoing evolution of



security technology for retail ATMs designed to meet constantly evolving threats. So paramount is this reality in our industry that the majority of exhibitors at NAC's annual conference this past fall addressed some aspect of ATM safety/security in their product offerings/booth displays. Given the pace of technological change in this sector alone, it is highly impractical and unwise to attempt to legislate and bind ATM owners and operators to current security measures which are likely to become technologically outdated or even counterproductive in very short order.

Retail ATMs first came into being in the mid/late 90s, prior to which time all ATMs in the U.S. were bank owned/operated. Back then, there were only approximately 120K ATMs in the U.S. However, since entry of America's entrepreneurs into the business, the U.S. ATM base has grown three-fold to well over 400K ATM terminals providing convenient access to cash throughout the USA. These new retail ATMs came into precisely those areas least/not served by bank ATMs, where access to cash was needed, including for our most unbanked/under-banked citizens. Retail ATMs now represent the great majority of all ATMs in America and in New York.

Unfortunately, many of America's retail ATM providers are under serious economic and operational pressure today from a variety of sources, particularly increased network fees and the significant costs/exposures from EMV chip card implementation at their ATMs. Given this state of affairs, the initial and ongoing costs of compliance from the new regulatory regime/requirements that would be imposed by Int. 1406-2016 are potentially devastating for NYC ATM providers, merchants and the consumers they serve. If enacted, the unintended results of such an ordinance will almost certainly be far fewer retail ATMs and/or higher ATM fees for consumers, with no measurable offsetting improvements to ATM safety or security within the City.

Should New York citizens have to go searching because cash is no longer readily available at the local convenience store, when they need it quickly to pay the day care provider or babysitter? How about the tourist mugged at an outdoor bank ATM because there is no longer an ATM in the very public and safe interior hotel location? How about the enormous loss in impulse sales and the associated tax base for the City from all the purchases that go unmade because convenient cash is no longer available at the neighborhood bodega? Please carefully consider the many detrimental consequences this ordinance would have on NYC ATM businesses, retailers, and the public we are privileged to serve.



What the Council Can Do to Help

Although the current ordinance is impractical and will not help as desired, there are important and constructive things the Council can do that will enhance safety at NYC ATMs. Specifically, we would ask that the City work to implement a stronger penal code and enforcement for ATM related crimes and help us lobby for this same result in Albany. We would also ask that you consider providing additional support for law enforcement to work more closely with the ATM industry in preventing these crimes and catching the criminals. And, as the trade association that exclusively represents the independent ATM business in the U.S., we will continue to provide top quality education and resources for these businesses regarding ATM safety and security.

Fundamental Problems with the Proposed Ordinance

The Proposed Ordinance would chill ATM placement & make it too costly and difficult to maintain or place new ATMs in many locations.

- “One-size-fits-all” – simply doesn’t work for the myriad of different real world retail ATM locations and specific circumstances.
- Regulatory Overkill – The industry can’t contend, administratively or cost-wise, with multiple regulatory schemes for each different municipal local jurisdiction in which ATMs operate.
- State Preemption – last year’s ATM Safety Act adopted by the NY state legislature expressly carved out retail ATMs from many of the very same requirements that the Proposed Ordinance seeks to now apply. There were good and valid reasons retail ATMs were carved out of the ASA, consistent with this testimony. Passage of the proposed ordinance would run directly counter to exemption provided under governing state law.
- Federal Preemption – the requirements of the proposed ordinance will have a material adverse affect upon the retail ATM business in NYC that conflicts with applicable federal law and regulations governing the ATM business. This interference with interstate commerce is preempted and would be held invalid if challenged.



9802-12 Baymeadows Road, #196 | Jacksonville, FL 32256 | O (904) 683-6533 | F (904) 425-6010
EMAIL mail@natmc.org | WEBSITE www.natmc.org

- Equal Protection – the ordinance is discriminatory by targeting bank sponsored ATMs versus treating all “off-bank-premise” ATMs equally. The basic premise of the ordinance that there are “non-bank” ATMs is factually incorrect and is an unsound foundation upon which to proceed.
- Violates Contracts Clause of US Constitution – certain requirements of the Proposed Ordinance addressing ATM placement contracts represent an unconstitutional interference with private party contractual rights under the United States Constitution.

For all these reasons, The National ATM Council, Inc. respectfully requests that Int. 1406-2016 be tabled at this time, and that the Committee work with NAC and other interested parties to develop appropriate revisions to the penal code and enforcement protocols that will actually help deter ATM related crimes and protect New York’s consumers of ATM services.

Respectfully Submitted,

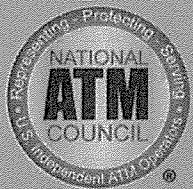
THE NATIONAL ATM COUNCIL, INC.

By: Bruce Wayne Renard
Bruce Wayne Renard, Executive Director

CC: NAC Board & Officers

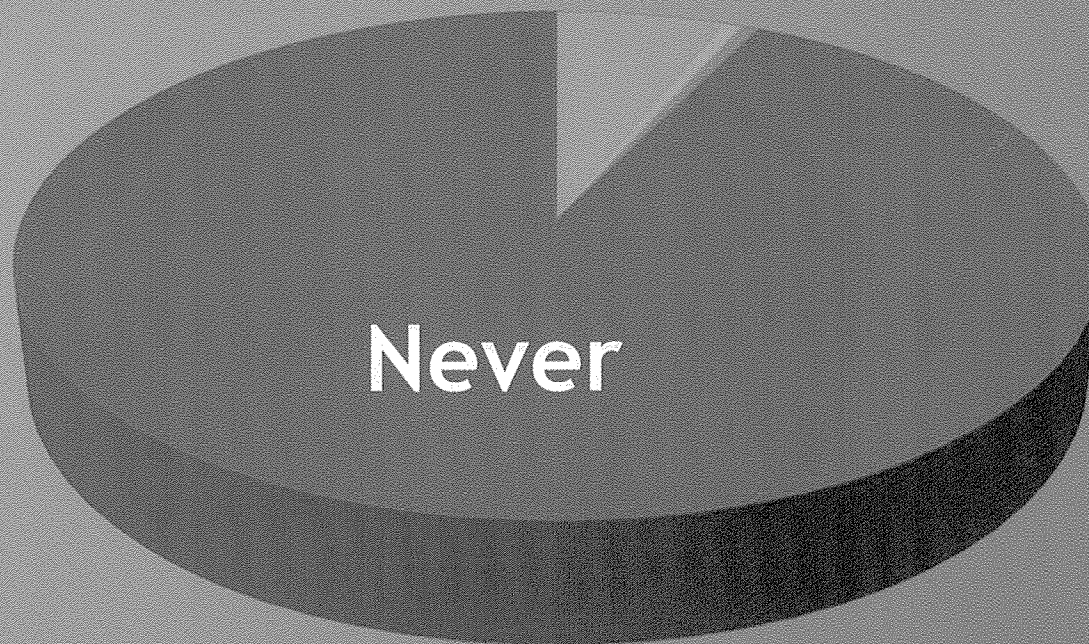
U.S. Retail ATM Skimming Survey 2016

A brief study of skimming activity as reported
by U.S. independent ATM deployers



How many times have you found/removed skimming devices at your ATMs?

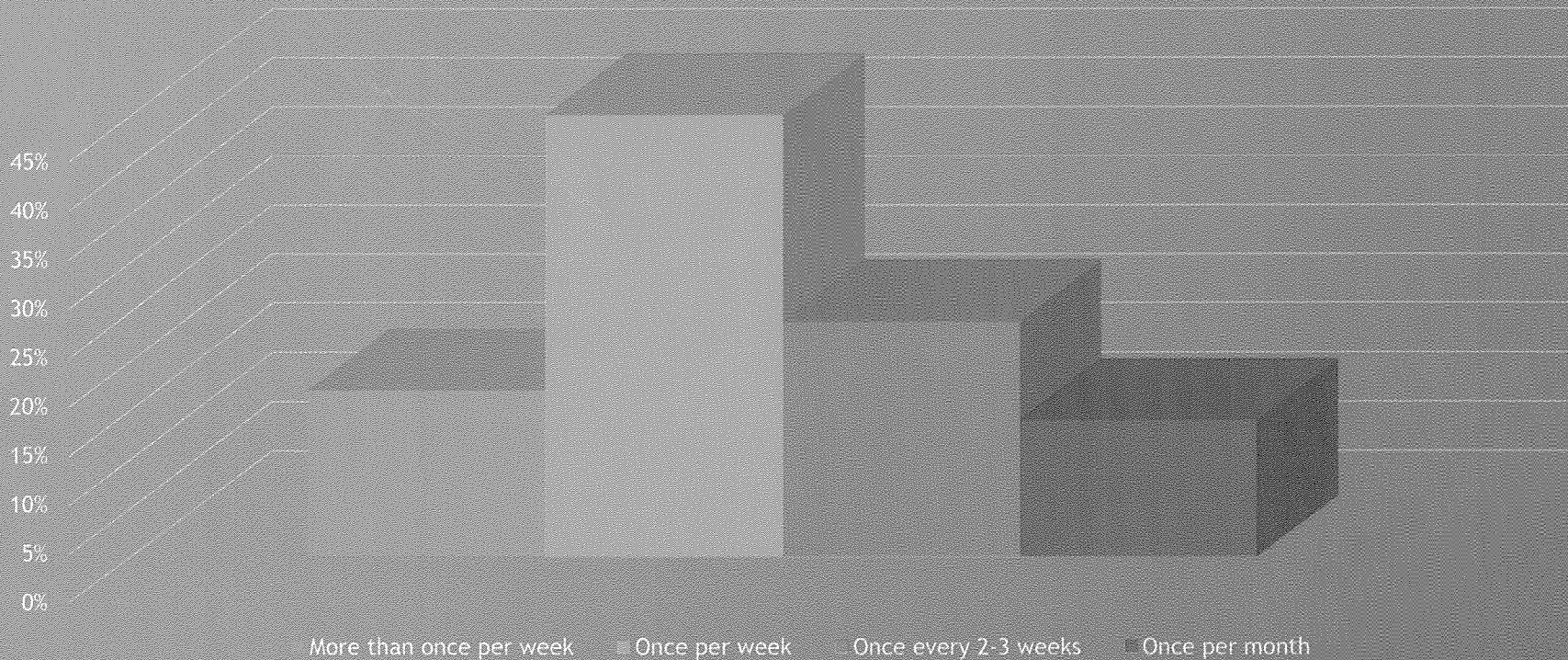
#1



1-5 Times 6-10 times More than 10 times Never

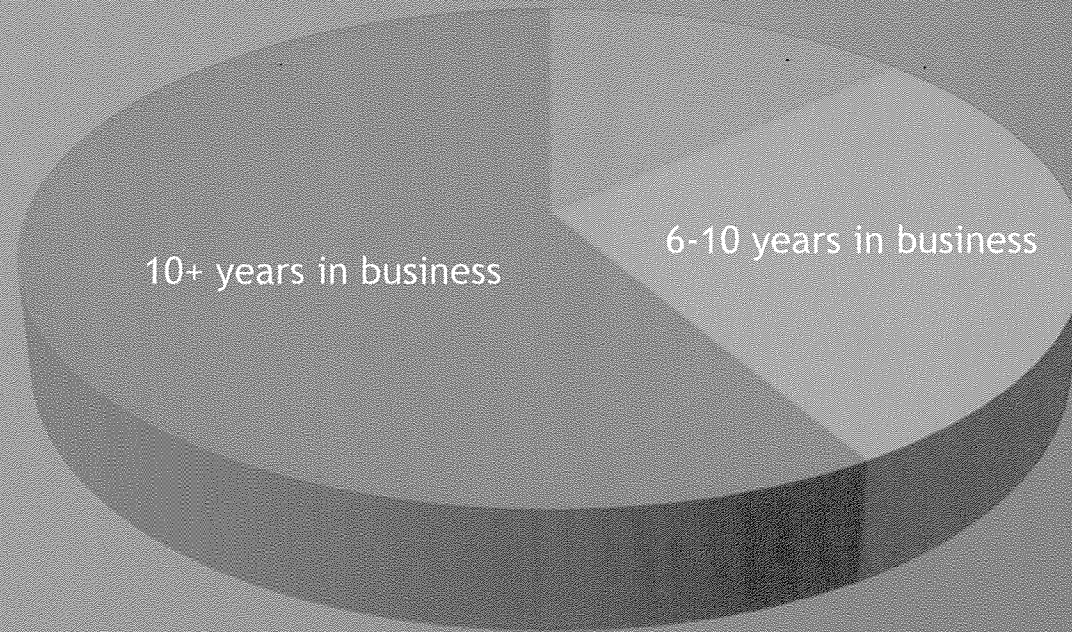
How often do you inspect your ATMs - where you would be able to detect a skimming device?

#2



How long have you been in the ATM business?

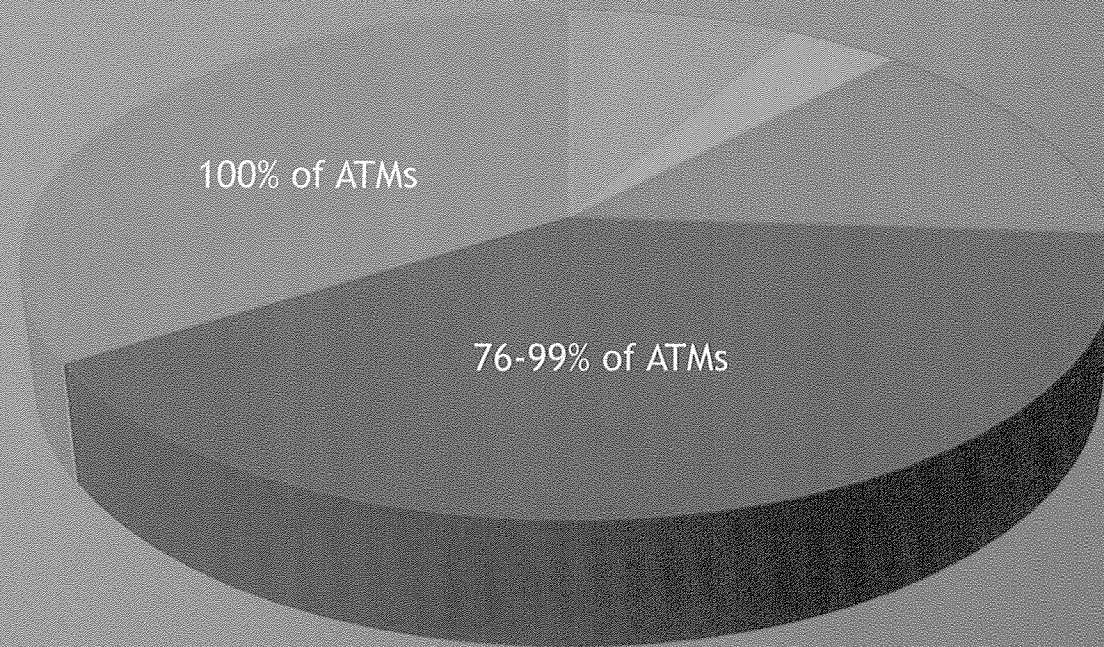
#3



■ 1-5 years ■ 6-10 years ■ 10+ years

What % of your ATMs are in locations manned by store personnel who are present and able to observe the ATM during the times it is available for use?

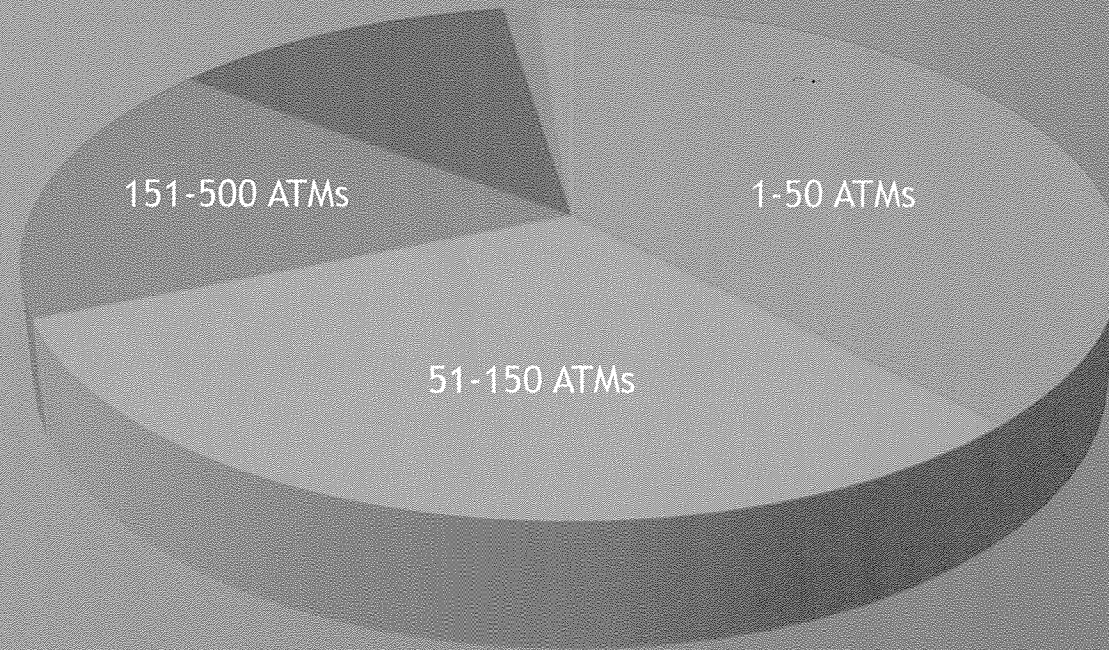
#4



■ 25% ■ 26-50% ■ 51-75% ■ 76-99% ■ 100%

How many ATMs do you own, operate or manage?

#5



1-50 51-150 151-200 500-2,000 2,000-5,000 Over 5,000

Survey Details

Survey conducted by The National ATM Council, Inc. 4/26/2016 - 5/25/2016
Based upon 166 random responses from U.S. Retail ATM Owners and Operators

For more information contact NAC at: 904-683-6533 or email: mail@natmc.org



Skimming Detection & Deterrence *for Convenience Store ATM Owners*

What is ATM Skimming?

Skimming is the theft of credit/debit card information by a device placed in, on, or around an ATM. These devices allow criminals to secretly record credit/debit card information (from the magnetic stripe) - for later use in fraudulently producing counterfeit cards. ATM skimming also includes capturing customer PINs associated with the cards using a hidden micro camera that records the PIN digits. Keypad overlays and "shoulder surfing" are other methods.

What is the Skimming Threat for My Store ATMs?

Although convenience stores and other indoor retail ATMs have traditionally not been targeted by criminals, skimming now appears to be on the rise as criminals sense a "closing window of opportunity" with the new and more secure EMV chip cards and EMV updated terminals now being implemented in the U.S.

It's very important to know how to detect and deter skimming at your store ATMs in order to continue providing a safe environment for your customers. This Guide outlines steps you can take to help stop skimming and what to do if/when your ATM is ever compromised by a skimming device.

What Can I Do To Maintain and Maximize a Safe Environment for My Store ATMs?

There are several steps you can take to help reduce the threat of skimming at your store(s):

- **Place your ATM where it can be seen by your cashier AND make sure your video surveillance covers the ATM**
Place an ATM in store locations where it: (i) will not be needlessly exposed to "smash & grabs"; (ii) is under line-of-sight visual surveillance by store personnel; and (iii) does not expose communications cables or other points of entry/exit to the ATM's components or communications. Be sure your video surveillance captures the face of the person using the ATM and not PIN entry or display screen information.
- **Train your employees**
Use this Guide as a key part of training employees. Keep a copy at the cash register for easy reference, but be careful to keep it secure, out of sight, and accounted for at all times.
- **Know your ATM**

You and your employees should familiarize yourselves with exactly what the ATM(s) in your store(s) look like without any skimming devices installed. Take photos of

the ATM so you have a comparison for reference. Remember, criminals are very good at making skimmers look like they "belong" - so a good mental and physical image of your unaltered ATM is important when making the regular inspections needed to detect skimming.

- **Inspect your ATM on each shift or at least once a day**
Each shift manager should perform an ATM inspection. This takes only a short time, but is perhaps the most important element in a comprehensive anti-skimming program.
 - > There are two basic categories of skimming devices: internal and external. External skimmers are placed on the outside of the card slot - on top of the ATM card reader. Internal skimmers are placed inside the card slot and are more difficult to detect. You should be checking for both types of skimmers.



Internal ATM Card Slot Skimmer

> Examine your ATM card reader.

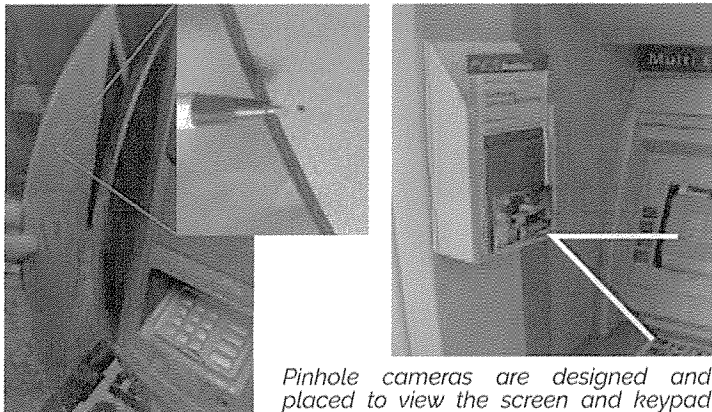
Check the card reader opening by jiggling/pulling on the card reader itself. It should be solid and not move. Most skimmers are temporarily installed with double-sided tape and will come off easily if pulled. Look inside the card slot to see if any device has been placed within the normal space, or if anything looks "different" in the size or shape of the card slot. Push a non-functioning card, such as a non-activated gift card, into the slot to test whether the card goes in smoothly, or feels "different" - indicating an internal skimmer has been installed.



External ATM card reader overlay skimmers are designed to look very similar to the machine's card reader - but have minor differences that are recognizable if you know your machine.

> **Look for a micro camera.**

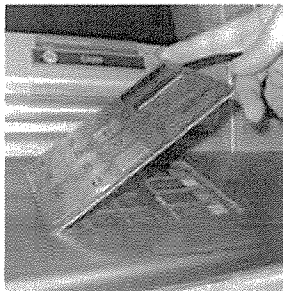
Cameras used by criminals are tiny and usually hidden in items such as a literature holder or disguised as a component of the ATM enclosure itself with line of sight to the keypad.



Pinhole cameras are designed and placed to view the screen and keypad simultaneously.

> **Inspect for a keypad overlay.**

These go right on top of the ATM key pad and are normally secured with double-sided tape. Again, jiggle and "pressure test" the key pad. Look for a lip around it that wasn't there before. Look closely and notice whether the color, texture, etc. are different.



PIN Pad Overlay

> **Inspect for internal skimming device.**

If you have authorization/access to the interior of your ATM, check for an internal skimming device. Internal devices include those placed inside the ATM cabinet and connected directly to the card reader or to the computer board that controls the card reader/captures the card data. These and other skimming devices may have Bluetooth wireless capability to transmit stolen card data to criminals. Request that your ATM service provider/vendor show you exactly what to look for -- and then incorporate an internal examination into your regular ATM anti-skimming regime.

> **Use Bluetooth/Wi-Fi Scanners.**

Use one of the free Bluetooth/Wi-Fi scanner apps available for most smart phones to regularly scan for any new/unrecognized signals/devices. Run a "baseline" scan of your store, making note of the "normal" signals/networks/devices, so you can detect any changes in subsequent scans.

What Other Protective Steps Should I Take?

Check with your ATM vendor about available anti-skimming devices for your ATM(s) – to thwart ever more sophisticated skimming techniques and devices from the criminals. These devices range from physical attachments constricting card slot entry to newer card readers with embedded anti-skimming electronics that detect/alert you to placement of a skimmer, and may emit "jamming signals" and encrypt card data.

What Should I Do Right Now?

As an important first step, contact local law enforcement now, before a skimming incident occurs, and ask for advice on their preferred course of action in the event you do find a skimming device on your ATM. Write down the instructions and let your ATM vendor/service provider know of this local protocol for their feedback and confirmation. Follow the steps outlined by local law enforcement wherever possible.

What Should I Do To Educate My Customers?

Use the ATM screen display and physical signage to remind your customers to always cover the key pad and their finger movements with the other hand when entering their PIN. This simple step is key to keeping customers' most sensitive information safe.

What Should I Do If I Find a Skimming Device In/On My Store ATM?

1. Be careful not to touch the skimming device itself, but immediately place an "Out of Order" sign on the ATM. Follow the protocol provided to you by local law enforcement - including contacting them immediately to advise of a skimming device found on your ATM. Ask them to come to your store so they can obtain evidence and you can file a report. (You may also wish to contact your closest regional US Secret Service office.)
2. Contact your ATM vendor immediately and let them know you believe you have found a skimming device on your ATM. Let them know you have also contacted law enforcement and ask your ATM vendor to coordinate with them to ensure the safe/secure removal of the skimmer and restoration of the ATM to normal service. If you "self-service" the ATM, and local law enforcement does not arrive promptly (within 2-3 hours where the ATM is critical to your business), follow these steps before restoring the ATM to service:
 - > Take photos of the skimming device as installed.
 - > Remove the device with as little handling/destruction as possible, using protective gloves if available.
 - > Store the skimmer/camera in a plastic bag to provide to law enforcement whenever they arrive.
3. Be alert to notice if there is a car/truck parked nearby for long periods of time. Bluetooth wireless can be used to retrieve card data from nearby skimming devices in real time. If you see someone suspicious, make a good mental note and discretely record the license plate/make/model/color/departing direction of travel and provide that information to the authorities.
4. If you observe a person attempting to recover the skimming device, DO NOT INTERVENE. Discretely note and write down the physical features of the person(s), their clothes, car/truck license plate number/make/model/color and direction of travel, and provide to law enforcement ASAP once the suspect leaves.

Version 01 / Effective 08/19/2016



CONFIDENTIAL - FOR NAC MEMBERS ONLY

New York ATM Skimming Attacks

This is to notify our members who operate in the Greater New York Metropolitan Area of current skimming crimes being experienced by some of our ATM operator members in NYC. This skimming scourge is believed to be the work of a Russian organized crime group and is being taken very seriously by the N.Y.P.D.

These recent skimming devices are sophisticated and well disguised. Here are two examples of skimmers just found on terminals in the New York area.



As can be seen from these photos, the skimmer and pinhole camera are made to look/fit seamlessly onto the regular ATM unit. These devices are applied with two-sided tape and can be quickly and easily placed on your ATM (and also readily detected/dislodged by jiggling/pulling on them).

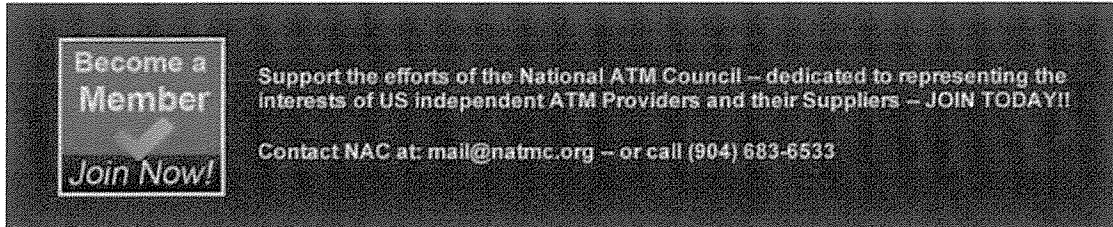
You should notify all your location operators and owners to be on high alert and check daily for this form of attack - and to contact you immediately if they find a skimmer on their ATM.

If you encounter a skimmer placed on one of your ATMs in the NYC area, please promptly contact NAC Board Member/New York operator George Sarantopoulos at (646) 739-2660. George is helping spearhead our industry liaison with N.Y.P.D. and can help ensure the quickest/most effective police response to the location.

As you know, retail ATMs have been spared from most of the skimming incidents of the past - which have focused much more on bank ATMs. Experience in other countries has shown, however, that a spike in this type of card fraud is likely once EMV implementation gets underway -- presumably because the criminals see a closing window in which to use their fraudulently obtained mag-stripe data.

As such, at this critical time, ATM owners/operators in NYC and elsewhere across the U.S. must be extremely vigilant when it comes to skimming - and educate their retailers/merchants to be on high alert for attempted skimming at their ATMs over the next 12-18 months. NAC wants to help the industry stay on top of this threat - so please let us know if you encounter skimmers on your ATMs anywhere in the U.S. - and we will continue to alert you to any major new skimming developments.

Let's show these crooks that independent owners/operators will not be deterred from safely and securely providing cash to the U.S. public. Thank you!



Become a Member
Join Now!

Support the efforts of the National ATM Council – dedicated to representing the interests of US independent ATM Providers and their Suppliers – JOIN TODAY!!

Contact NAC at: mail@natmc.org – or call (904) 683-6533



ATMs ACROSS AMERICA **NAC2016** 17 - 20th OCTOBER

A New Frontier

Buena Vista Palace, a Hilton Affiliate
© Walt Disney World



The National ATM Council, Inc., 9802-12 Baymeadows Rd. #196, Jacksonville, FL 32256

[SafeUnsubscribe™ {recipient's email}](#)

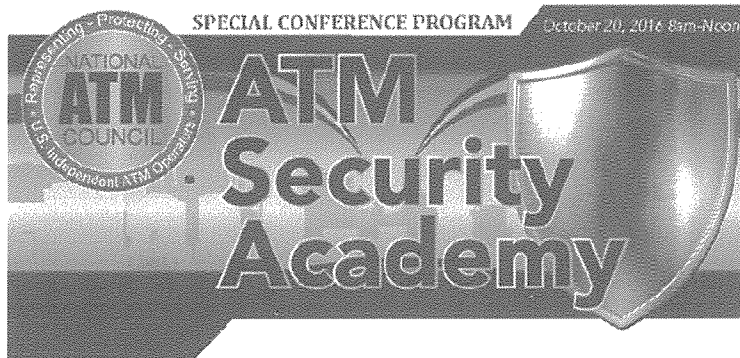
[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by bruce@natmc.org

Thursday, October 20, 2016

8:00am - 1:00pm Registration Desk Open

8:00am - Noon **ATM Security Academy** [Great Hall West]



Inaugural Breakfast
Sponsored by:



Welcome

- Bruce Renard, Executive Director, National ATM Council
- Stephen Joseph, Business Development Manager, Banking & Finance, Axis Communications; NAC Conference Committee, Security Academy Chair



NAC2016 ATM

ATM Equipment Security

Moderator:

- Tim Baxter, President, SwypCo LLC

Panelists:

Physical Placement of the ATM

- Glade Jones, Operations Manager, eGlobal ATM
- Jason Kuhn, VP Product Marketing & Planning, Nautilus Hyosung
- John MacDougall, VP Customer Support, Genmega
- Mike Nelson, VP Business Development, Payment Alliance International
- Derek Smith, President, Eclipse Cash Systems

Electronic Security Considerations

- Stephen Joseph, Business Development Manager, Banking & Finance, Axis Communications

Skimming Detection/Prevention Strategies & Cyber Protection

- Glen Gulyas, CEO, Onclave Networks, Inc.
- Russ Hinely, National Account Manager, ACG
- James Phillips, VP of Sales & Marketing, Triton
- Bruce Renard, Executive Director, National ATM Council

ATM Cash/Personnel Security

Moderator:

- Larry Scott, President, CTI

Panelists:

- John Gibadlo, U.S. Eastern Region Sales Manager, 3SI Security Systems
- Cliff Jordan, Chair, IACOA; President, Rapid Armored Corporation
- Robert Lynch, SVP National Financial Business Development, Loomis



Security Academy

Insurance/Risk Mitigation Considerations

Presenters:

- Brad Moody, CFI, CFE, EVP Operations, Lowers Risk Group
- Mike Salzillo, Sales Executive, Marshall & Sterling Insurance

Special Guest Presenter:

Vito Roselli, Supervisory Special Agent,
Violent Crimes Unit of the HQ Investigative Division,
Federal Bureau of Investigation

A graduate of the U.S. Coast Guard Academy in 1988, Special Agent Roselli spent nine years in law enforcement operations before joining the FBI in 1997, where he was assigned to the Philadelphia Division. During this tenure, Special Agent Roselli fought violent/gang related crimes and served two special intelligence mission support deployments in Iraq.

Supervisory Special Agent Roselli began his tenure at FBI Headquarters in Washington, DC in May of this year, where he currently serves as Program Manager for the FBI's nationwide violent crime program.

**Testimony of Michael E. Keller, Co-Chair ATMIA Government Relations Committee,
To the NYC Council Committee on Consumer Affairs
Regarding NYC Council Intro 1406-2016
January 12, 2017**

Re: Int 1406-2016: Requiring certain security measures at nonbank ATM

Good morning, Chairman Espinal and members of the Committee. Thank you for the opportunity to testify today on Intro 1406 related to ATM safety.

My name is Michael Keller. I am Co-Chair of the Government Relations Council of the ATM Industry Association (the "ATMIA"). ATMIA is an independent, non-profit trade association, engaged in non-competitive promotion of the ATM industry. Its mission is to promote ATM convenience, growth and usage worldwide; to protect the ATM industry's assets, interests, good name and public trust; and to provide education, best practices, political voice and networking opportunities for member organizations. Those members include scores of merchants and ATM service vendors in the greater New York City area.

I am here to raise ATMIA's concerns regarding Intro 1406-2016 and to offer you our assistance in regard to a better understanding of the ATM industry.

It is our understanding that the impetus for this legislation is to curtail or eliminate the skimming of ATMs. When an ATM transaction is skimmed, the skimmer obtains only the card number and, if a video recorder is also installed, the consumer's PIN. With this data, skimmers can create a counterfeit debit card (commonly known as a 'white' card) that can then be used at another ATM located anywhere in the world to make a cash withdrawal.

However, it is important to note that the captured or skimmed data is insufficient to enable the skimmer to steal the identity of the cardholder or to use the cardholder's credit for his or her benefit. Further, if a consumer's ATM debit card is skimmed and thereafter a white card is used to withdraw cash from the consumer's account, federal regulations (commonly known as 'Reg E') require the consumer's bank to refund in full the wrongfully dispensed cash so long as the cardholder submits a request to their financial institution within sixty (60) days of the transaction.

Of course, skimming also takes place at other electronic payment platforms such as gas station pumps, point-of-sale terminals, and even in restaurants and other retail establishments where portable skimming devices are deployed. ATMIA supports the Council's goal of defeating skimming. However, skimming is a national and international problem that requires a national/international approach. To date, the electronic payments industry has implemented many anti-skimming measures, such as EMV technology, PIN shields, physical inspection of ATMs, anti-skimming mechanisms, monitoring, and education. The ATMIA has supported these measures through the publication of 'Best Protection' education materials and is continuing to seek out other opportunities to defeat skimming. We appreciate the Council's interest in this issue and offer our comments to your proposed legislation.

To facilitate your review, our comments regarding the proposed legislation follow the order of the seven sections of the legislation.

Section 20-699.7 Definitions. At this time, the ATMIA has no comments regarding the six (6) defined terms in this section. We reserve the right to submit further comments should additional definitions or if new or revised provisions are added to the proposed legislation.

Section 20-699.8 Placement Agreement. ATMIA agrees that a written placement agreement should be in place with regard to each nonbank ATM. In fact, it is our understanding that virtually 100% of nonbank ATMs are covered and affected by a written placement agreement. We do have concerns regarding Subsection 2 (Placement of nonbank ATM) of this section. Specifically, we do not believe it is necessary for Subsection 2 to require that the placement agreement “shall identify the specific point within the location or premise.” In the vast majority of placement agreements and in particular within the greater NYC area, the location or premises on which a nonbank ATM is placed is usually a relatively small space, i.e. a few hundred square feet. For that reason, ATMIA does not believe that the placement agreement needs to “identify the specific point”, but only to refer to the address at which the ATM is to be located.

Section 20-699.9 Security measures. With regard to Subsection ‘a’ (Surveillance camera), the ATMIA is confused by the phrase “all persons entering a nonbank ATM located within the interior of a building”. Since no one can ‘enter’ a nonbank ATM, we respectfully submit that this phrase should state: “all persons entering the establishment at which a nonbank ATM is installed.”

With that suggested clarification, the ATMIA believes that a merchant who has installed an ATM within the interior of the business need not have a surveillance camera focused on the ATM. If NYC sees fit that all retail establishments must have a video camera recording each customer entering or leaving that establishment without regard to the presence of an ATM, the ATMIA has no objection to such a measure; but does object to targeting only those merchants that have a nonbank ATM within their premises. Aside from the frequency of inspection, we also have concerns about “inspections” being conducted by people who are not trained to detect the evolving technologies used by professional criminals to harvest ATM card information. Accordingly, we do not believe surveillance cameras focusing on the ATM will have a material deterrent effect on skimming activities, which is done primarily by well-trained gangs.

With regard to the ‘Adequate lighting’ provisions of this section, the ATMIA reserves its comments until such time when we are able to consult with ‘lighting’ professionals or technicians who can explain to us what, if any, special equipment, may be required to satisfy the prescribed lighting requirements.

The “periodic inspection” requirement set forth in Subsection ‘c’ is very problematic. Setting the ‘minimum frequency’ of inspection at once every 24 hours is very onerous. It

suggests that any merchant who wants to do more than the ‘minimum’ will be inspecting the ATM more than once every 24 hours—perhaps hourly.

The term “ATM” stands for an ‘automated teller machine’. The economic viability of an ATM is derived from its ‘automated’ nature. Requiring a merchant or a distributor to inspect the ATM at least daily severely increases the cost of operating that ATM. For that reason, we request that the frequency of ATM inspections be changed to ‘each time the ATM is replenished with cash or otherwise receives any maintenance service.

We have no objection with the requirement that if a skimming device is discovered, that it be reported to the local police precinct.

Section 20-699.10 Exemptions. We do not understand why ATMs owned or operated by or for a federal or state bank are exempted from this legislation. Those ATMs suffer as much, if not more so, to skimming attacks than nonbank ATMs. To exempt them from this legislation provides them a competitive advantage over nonbank ATM owners/operators.

Section 20-699.11 Banking regulations. Please see our comment to Section 20-699-10.

Section 20-699.12 Penalties. Predicated on the adoption of our recommendations set forth above, ATMIA has no comments on the proposed penalties.

Section 20-699.13 Rules and regulations. No comment.

Section 2—Date law takes effect. Since virtually all nonbank ATM placement agreements are currently covered by written ATM placement agreements and there are several thousand such agreements that will be covered by this proposed legislation, ATMIA respectfully suggests that the effective date of this proposal be not less than one year after enactment so as to allow sufficient time for the thousands of affected merchants and ATM distributors to comply with the terms thereof.

Once again, thank you for the opportunity to provide our testimony. We look forward to working with you to protect all consumers. I am available to answer any questions you may have.

##

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Jim SHRAYET

Address: 66 John St

I represent: North East ATM ASSOC

Address: 66 John St.

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Robert Taichman

Address: 280 85th Street

I represent: Access card ATM

Address: _____

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Peter Wilkensloff

Address: 111 Plainfield Ave, Floral Park NY

I represent: Best Products

Address: same

Please complete this card and return to the Sergeant-at-Arms

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 1406 Res. No. _____

in favor in opposition

Date: 1-12-17

(PLEASE PRINT)

Name: Abc Ayesh

Address: _____

I represent: ATM World

Address: 3342 97th St

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

1406

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: 1/12/2019

(PLEASE PRINT)

Name: George Sarantopoulos

Address: 280 84th St, Brooklyn, NY 11209

I represent: Access One

Address: 280 84th St, Brooklyn, NY 11209

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 1406 Res. No. _____

in favor in opposition

Date: 1/12/19

(PLEASE PRINT)

Name: Casey Adams, Deputy Dir. of City Legislative Affairs

Address: 42 Broadway

I represent: NYC DCA

Address: 42 Broadway

Please complete this card and return to the Sergeant-at-Arms

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

[]

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: 1/12/15

(PLEASE PRINT)

Name: Mart Cooley, Assistant Commissioner

Address: 42 Broadway

I represent: NYC DCA

Address: 42 Broadway

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

[]

I intend to appear and speak on Int. No. 1406 Res. No. _____

in favor in opposition

Date: 1/12/17

(PLEASE PRINT)

Name: John Spina, First Deputy Commissioner

Address: 42 Broadway

I represent: NYC DCA

Address: 42 Broadway

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

[]

I intend to appear and speak on Int. No. 1426 Res. No. _____

in favor in opposition

Date: 1/12/17

(PLEASE PRINT)

Name: James Hurst, Director of Enforcement

Address: 42 Broadway

I represent: NYC DCA

Address: 42 Broadway

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. 1406

in favor in opposition

Date: _____

Name: Robert Reichman (PLEASE PRINT)

Address: 210 E. 15 St

I represent: ATM industry

Address: _____

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

in favor in opposition

Date: _____

Name: Bruce Renard (PLEASE PRINT)

Address: 9802 - 12 Baymeadows Rd #196

I represent: JAY FL 33356
The National ATM Council, Inc

Address: SAME

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 1406 Res. No. _____

in favor in opposition

Date: 1/12/17

Name: MIKE KELLER (PLEASE PRINT)

Address: _____

I represent: ATMIA + CARDTRONICS

Address: _____

Please complete this card and return to the Sergeant-at-Arms