



October 23, 2013

Criminal Justice Committee; Michigan House of Representatives

Dear Committee Members:

Good morning, my name is Stephen Dedene. I am the Manager of Compliance and Regulatory Affairs for Credit Union ONE. Credit Union ONE is a state chartered credit union founded in 1938 and headquartered in Ferndale with 17 branches in the Metro Detroit, Grand Rapids, and Traverse City regions. Credit Union ONE has over 106,000 members and over \$800 million assets.

I would like to thank the committee for the opportunity to testify today regarding ATM skimming and House Bills 5050-5054. I am here today in support of House Bills 5050-5054 and to provide background on the increasing ATM skimming trend, and its impact on consumers and financial institutions, specifically Credit Union ONE.

Skimming is a type of fraud that occurs when thieves steal information from a consumers ATM, debit, or credit card and use this information to make fraudulent cards. These fraudulent cards can then be used to steal money from card holders and ultimately the financial institution of the consumer. Skimming occurs at the ATM when a device, which is for the most part undetectable, is installed over the card reader at an ATM machine. Additionally, either a keypad overlay is installed over the ATM keypad, or a tiny camera is hidden somewhere on or near the ATM machine. The keypad overlay and camera is used to capture the consumer's personal identification number (PIN) needed to conduct a transaction at the ATM machine. The skimmer and camera is usually left on the machine for no more than 6 hours and captures information on all users of the machine in this time period. Installation and removal of these devices takes mere seconds. Losses associated with ATM skimming vary from expert to expert with some experts, including the secret service, estimating losses at or in excess of \$1 billion annually.

When a consumer uses an ATM machine that has had skimming devices attached to it they are providing the thief with all of the information necessary to create a duplicate fraudulent card. When the consumer inserts their card into the card reader, the skimmer captures bank account information located on the card (the black magnetic stripe). They are stealing this information. This information is either stored on the device or sent electronically to a secondary device controlled by the thief. When the consumer enters their pin number the hidden camera will capture their PIN or the keypad overlay will record the numbers entered in by the consumer.

While all of this is happening the consumer has no idea that their information is being stolen. The consumer ends up completing the transaction and the thief will have obtained their ATM, debit, or credit card information, as well as their PIN number. The thief will then use this information to create fraudulent cards. Some of the most sensitive information an individual has is now compromised.

Fraudulent cards are created by simply taking the captured information and encoding it to a blank plastic card. Materials needed to skim and create the cards seem to be readily available over the internet. Once they have manufactured the fraudulent card the thieves can then spend at will. The thieves can now use the fraudulent card at ATM machines, grocery stores, online, gas pumps, restaurants, and pretty much any other place that accepts a card using the consumers' money.

In 2012 an ATM skimming ring in Oakland and Wayne County accounted for upwards of \$500,000 in fraudulent losses. Three of Credit Union ONE's ATM's had skimming devices installed on them between July and August. Hundreds of consumers (Credit Union ONE members, and non-members) who used these ATM machines while the skimming devices were attached had their information stolen. 85 of these members that had fraudulent cards used to withdrawal funds from their accounts were members of Credit Union ONE. Losses from 160 transactions totaled over \$91,000.

Despite the members suffering over \$91,000 in fraudulent activity they did not lose any money. The credit union reimbursed all 85 members the total amount they were victimized for, including fees. The monetary loss is actually suffered by the financial institution, in this case Credit Union ONE. Since Credit Union ONE is owned and operated by its members all members' share in the loss. This means that ATM skimming creates three victims, the member, the credit union, and the credit union's members'.

Since this incident the credit union has taken steps to help prevent further incidents of skimming. Shortly after the incidents in 2012 the credit union replaced the card readers on all of Drive-Up ATM machines. The new card readers will make the current skimmers incompatible with the new card reader. This will only last until the thieves modify the skimmer to fit the new card reader.

House Bills 5050-5054 will create and make much needed changes to Michigan Law. Current law does not specifically address ATM skimming; the possession, sale, or purchase of skimming devices; or jurisdictional hurdles associated with filing, investigating, and prosecuting. Sentencing guidelines are also inadequate for the type of crime being committed and can result in as little as 1 year and as much as 5 years in prison.

House Bill 5050-5054 will; amend state law to specifically address and define a skimming device, something that is does not exist today; amend the Michigan Penal Code by providing for penalties associated with skimming be tiered ranging from up to five years in prison and up to a \$25,000 fine for a first offense to up to 15 years in prison and a \$75,000 fine for third and subsequent offenses; prohibit the sale, purchase, installation, transfer, or possession of a skimming device; and solves jurisdictional hurdles in the case of multiple offenses in multiple jurisdictions by making any of those jurisdictions the proper jurisdiction for all of the violations.

It is my opinion, and that of Credit Union ONE, that House Bills 5050-5054 will protect and give a voice to consumers and financial institutions impacted by skimming by providing the necessary amendments to both serve as a deterrent from committing skimming crimes and ensuring that those suspected, tried, and convicted of these crimes will be punished in a manners that is sufficient for the type of crime they are committing.

Thank you once again for the opportunity to testify before you today and I respectfully ask for your support of House Bills 5050-5054.

Respectfully,



Stephen Dedene
Manager, Compliance and Regulatory Affairs
Credit Union ONE
248-584-5219
Stephen_dedene@cuone.org



The standard of trust.

October 7, 2013

Representative Kurt Heise
Anderson House Office Building
N-699 House Office Building
Lansing, MI 48933

RE: House Bill 5050

Dear Representative Heise:

We would like to thank you for the introduction of House Bill 5050 regarding Card Skimming. Card skimming is a faceless crime that affects many financial institutions and residents across the State of Michigan.

Recently, OMNI Community Credit Union was involved in a Card Skimming incident. This incident is still under investigation and no charges have been filed. The card skimming device was placed on our ATM in Oshtemo Township. The individual who put the skimming device onto the ATM was able to do so in about thirty seconds. We believe that the device was on the ATM for roughly twelve hours. So, with 30 seconds of work by the fraudsters: 27 individuals were affected; \$10,000 was out the door.

As a financial institution, fraud intervention is consistently on our mind. We stay up to date with the latest software and equipment that can be provided to prevent these sort of crimes from being committed. However, those who are out to commit these crimes always find a way around the newest technology.

The bill that you have proposed will be a good step forward in reducing the use of these skimming devices, by charging them with a felony as well as possible imprisonment and fines.

Should you require any additional information, please feel free to contact me at (269) 441-1447.

Regards,


Debi Southworth
Chief Lending Officer
OMNI Community Credit Union

ATM Skimming

Skimming is an illegal activity that involves the installation of a device, usually undetectable by ATM users, that secretly records bank account data when the user inserts an ATM card into the machine. Criminals can then encode the stolen data onto a blank card and use it to loot the customer's bank account.

1 Hidden camera

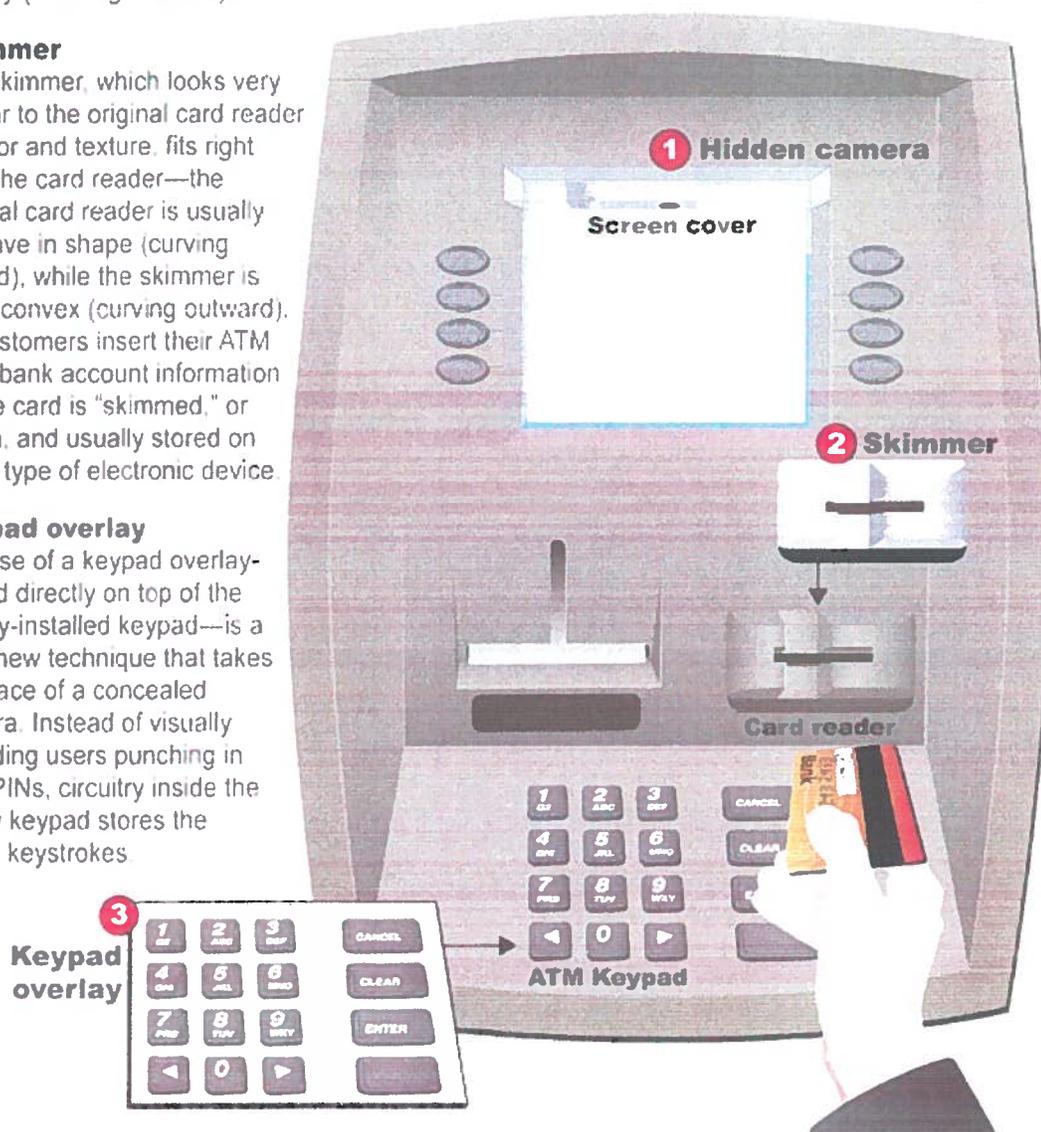
A concealed camera is typically used in conjunction with the skimming device in order to record customers typing their PIN into the ATM keypad. Cameras are usually concealed somewhere on the front of the ATM—in this example, just above the screen in a phony ATM part—or somewhere nearby (like a light fixture).

2 Skimmer

The skimmer, which looks very similar to the original card reader in color and texture, fits right over the card reader—the original card reader is usually concave in shape (curving inward), while the skimmer is more convex (curving outward). As customers insert their ATM card, bank account information on the card is "skimmed," or stolen, and usually stored on some type of electronic device.

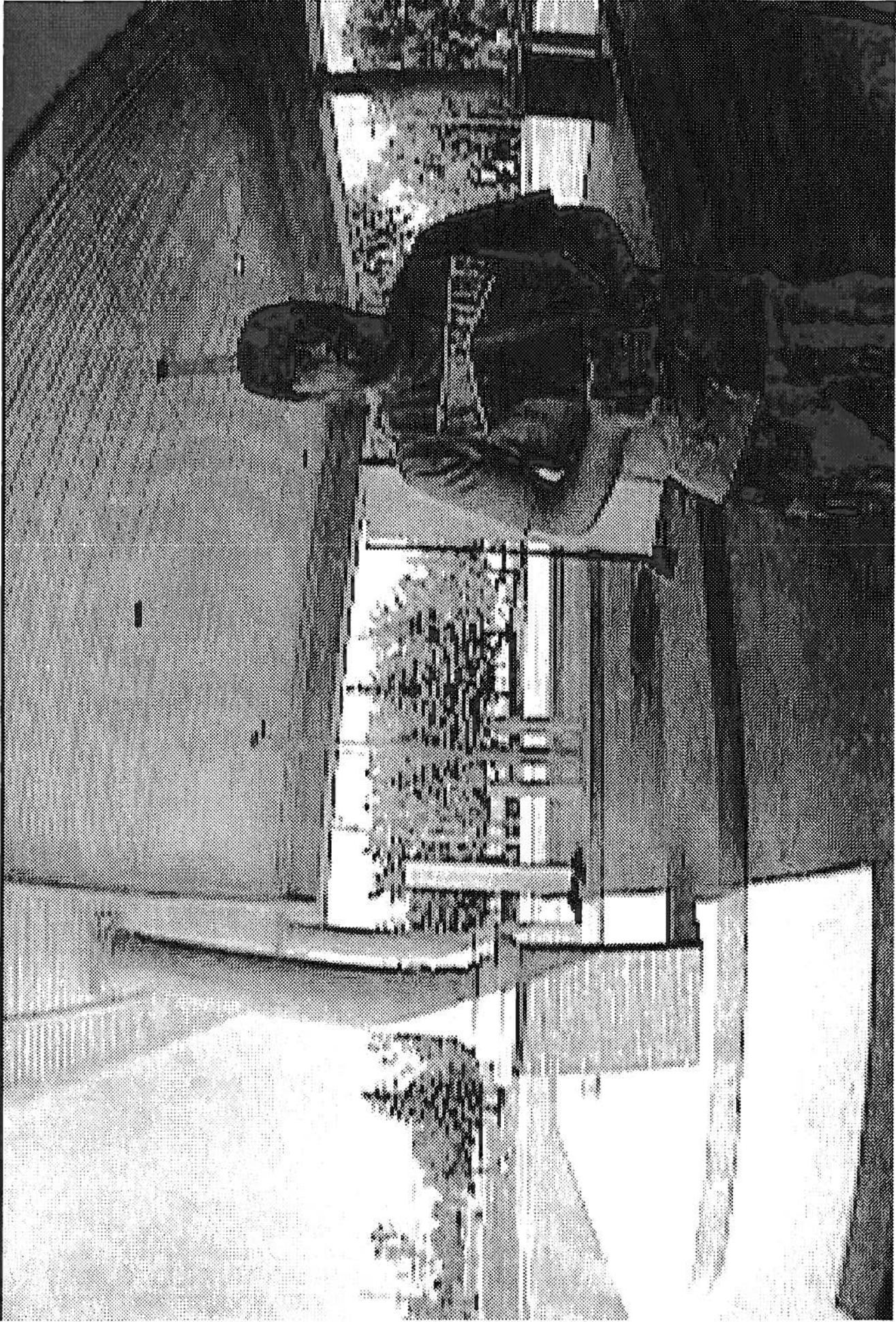
3 Keypad overlay

The use of a keypad overlay—placed directly on top of the factory-installed keypad—is a fairly new technique that takes the place of a concealed camera. Instead of visually recording users punching in their PINs, circuitry inside the phony keypad stores the actual keystrokes.





Divar name:	DIVAR-01	Camera input:	16
MAC address:	00-04-63-1E-19-2A	Unique ID:	67FF7704
Recording mode:	Continuous	Image size:	720(H) x 486(V)
Camera name:	ATM	Compression:	0.46 bpp
Date and time:	2012-06-24 02:54:33 PM	Image format:	4:2:2 wavelet compressed
Events:	Motion	Authenticity:	Image is authentic



Divar name: DVAR-01
MAC address: 00-04-63-1E-19-2A
Recording mode: Continuous
Camera name: ATM
Date and time: 2012-06-24 02:54:23 PM
Firmware: Mntian

Camera input: 16
Unique ID: 67FF765D
Image size: 720(H) x 486(V)
Compression: 0.49 bpp
Image format: 4:2:2 wavelet compressed
Authenticity: Imanto ic authentic