2019 SENATE INDUSTRY, BUSINESS AND LABOR COMMITTEE

SB 2262

2019 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Roosevelt Park Room, State Capitol

SB 2262
1/23/2019
Job #31275

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Amy Crane

Explanation or reason for introduction of bill/resolution:

Relating to the use and possession of re-encoders and scanning devices; to the unauthorized use of personal identifying information; and to the unlawful skimming of credit, debit, or other electronic payment cards; and to provide a penalty.

Minutes: Att. #1-3

Rick Clayburgh, President/CEO, North Dakota Bankers Association: Testified in support of the bill. We're here in support of the bill. The idea for the legislation came up at national meetings trying to address credit card fraud that occurs when skimming activity happens. If you're not familiar, it can be a situation at a gas pump or an ATM machine, criminals will put a device over the area where you put your card in. The skimming device will take the information off of the magnetic strip, and transmit it to somebody close by, if they do it at an instant cash machine, it will pick up the codes or pins that you put in. The crooks will put a blank card in an ATM and program your info onto the blank card. They now have all of your information. It's a crime to do that in North Dakota but it's not a crime to own a skimmer device. We're trying to address the issue of exploitation by giving another tool to the prosecutor's office. This bill will make it a class A misdemeanor, first time in possession, if you're caught with this in your possession and a felony for a second offence. We do this because someone may not be caught in the act but may have the equipment and the intentions to do so.

(3:44)Senator Piepkorn: Do you have an example of what the device is? What it actually looks like.

Rick: I just slip my card in and they have a little reader that can pick that up.

(5:04)Parrell Grossman, Director, Consumer Protection and Antitrust Division, Office of the Attorney General: see attachment #1 for testimony in support of the bill.

(13:08)Senator Burckhard: Let's say a server at a restaurant does this, is the business liable?

Parrell: I'm going to decline to say anything that my extent beyond my abilities as an assistant attorney general to do so. I would hate to commit liability to a restaurant or a business, that would be a decision for the impacted victim but I don't think it would automatically pose some kind of liability but I suppose there is always a possibility if they were aware of the conduct or reckless or some other thing that it could create some other concern but I will leave that for the private litigants.

Vice Chairman Vedaa: Why is it only a misdemeanor to possess?

Parrell: We weighed the egregiousness of possession compared to actually using it. At least we could envision someone in a relationship who gets the significant other to carry this unit, keep it in their apartment, have it in their vehicle. They don't necessarily use it but they do in fact possess it. In our minds, we thought that conduct was probably less harmful than just making something like that a felony. We just simply didn't want any unintended consequences we hope the legislature would send a strong message that these are not legitimate devices and there's no reason to possess them and maybe sanction them appropriately and we felt a class A misdemeanor was the right level.

Senator Piepkorn: Are there no legal uses or application for these devices?

Paraell: Nothing occurs to me but the whole idea is that it would be used to commit a crime. I can't think of an immediate use for this beyond to steal information. If there are any unintended consequences, we can address those in the future.

Chairman Klein: So you're saying that it would be unlikely that we would carry this in the backseat of our car for doing some kind of good?

Parrell: Well said.

Senator Piepkorn: Is there any responsibility for a gas station or some other retailer that possesses a machine that has a skimming device?

Parrell: I can't say about liability for businesses.

Chairman Klein: And that falls outside most of what we are discussing because most of that is kind of an internal waiter/waitress snitching of your personal information. How the merchant would be held responsible I think would be difficult to prove, but would you be able to tell if a restaurant would have that info?

Parrell: I think that is fairly prevalent for that kind of conduct to occur. Our financial institutions are very aggressive. And this is not limited to ATMs and gas station pumps

Chairman Klein: Do those issues come to you? When there is a skimming issue? So we can record that data? Do you know a number?

Parrell: I don't have a great answer; I am aware it happens on a regular basis but maybe less so than other states.

Vice Chairman Vedaa: Everybody should've gotten a video emailed to them, they drop that on there and they leave it on there for an extended period of time and then take it home and get all of the information and then go on to another place.

Parrell: Excellent point.

Senator Roers: Why aren't you attacking the manufacturers?

Parrell: That might be a little like the going after the people that create the devices that go after radar detectors. I wouldn't think that these types of devices aren't made here in the US so I would say these types of items are often confiscated by customs.

Chairman Klein: I was at a conference for alcohol policy when these vendors were talking about how easy it is to get fake ids made in China that now are so legitimate that they are impossible to tell if they are false. It's gotten to be business and it doesn't take much money.

(22:41)Barry Haugen, Independent Community Banks of North Dakota, (ICBND): See attachment #2 for testimony in support.

Senator Piepkorn: You said most of your members make good on the fraud, is it a requirement, to make good, is there a different between the institutions?

Barry: Yes, there is a difference. With our program, the credit card is provisional credit. There are insurance components to that, they still have to be reported in a timely fashion but that's generally not the problem. Debit cards get more difficult because that is an account with funds in it and there are some reporting requirements of the consumer. So there is some potential loss but in most cases our financial institutions make it right with them and the retailers probably do to.

(28:49)Mike Rud, NDPMA/NDRA: testified in support of the bill. As Parrell had mentioned, we'd been talking about this for 6 months just to strengthen the law. Last session in Iowa they passed some really strong skimming language. So we said what can we do to make this a better law for North Dakota and protect both the retailers and the consumers. And we think we've done that with this. I passed out some pictures for examples of what we're dealing with here (See attachment #3). We've had to put security seals on these pumps to try to offer our retailers some protection. We can buy these on the internet. The credit card scanners on the pump, this is becoming a huge concern, something needs to be done and we need to keep strengthening these laws. We're very excited that you're taking this to heart.

Chairman Klein: Gas pumps are probably the first of their kind like this, give us any inkling about how this has come to North Dakota?

Mike: I've heard of a dozen instances in which this has happened. These guys are working night and day to try to steal your money. Parrell and I've had enough discussion about this. This language will help us get out ahead of it.

Senator Burckhard: When I'm out pumping gas in my care and the wind is blowing and its 2 degrees, am I supposed to look for this stuff?

Mike: We've basically left it to our members to look for this stuff, to put the seals on their pumps. Unfortunately, not everybody is doing that, though.

Senator Burckhard: When you're at an ATM does anybody actually cover the pad?

Mike: I don't do it but you can see this device that's used on our ATMs, can read all those numbers. One of the things that we've run into in our industry is those locks on those pumps all had a universal key. And you can buy that key on the internet. So we've had to go back and all of our guys have changed their locks.

Chairman Klein: Similar to those pop machines out front of grocery stores.

Chairman Klein: Closed the hearing on SB 2262.

Senator Kreun: Move a Do Pass.

Vice Chairman Vedaa: Seconded.

A Roll Call Vote Was Taken: 6 yeas, 0 nays, 0 absent.

Motion carried.

Vice Chairman Vedaa will carry the bill.

Date: 1/23
Roll Call Vote #: 1

2019 SENATE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 2262

Senate Industry, Business and Labor Committee

☐ Subcommittee

Amendment LC# or Description: _____

Recommendation: ☐ Adopt Amendment
☒ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☐ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions: ☐ Reconsider ☐ _____

Motion Made By Kreun Seconded By Vedaa

Senators	Yes	No	Senators	Yes	No
Chairman Klein	X		Senator Piepkorn	X	
Vice Chairman Vedaa	X				
Senator Burckhard	X				
Senator Kreun	X				
Senator Roers	X				

Total (Yes) 6 No 0

Absent 0

Floor Assignment Vedaa

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

SB 2262: Industry, Business and Labor Committee (Sen. Klein, Chairman) recommends **DO PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2262 was placed on the Eleventh order on the calendar.

2019 HOUSE INDUSTRY, BUSINESS AND LABOR

SB 2262

2019 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Peace Garden Room, State Capitol

SB 2262
3/6/2019
33265

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Ellen LeTang

Explanation or reason for introduction of bill/resolution:

Use & possession of re-encoders & scanning devices, unauthorized use of personal identifying information & unlawful skimming of credit, debit or other electronic payment cards.

Minutes: Attachments 1, 2, 3

Chairman Keiser: Opens the hearing on SB 2262.

Rick Clayburgh~ND Bankers Association: This bill deals with two aspects. It deals with skimmers at gas stations or ATM's which takes your information & puts it on a new card. They are looking at making it a crime to own a skimmer or have it in possession & is a felony. This gives the law enforcement another tool.

Rep C Johnson: How do you get a hold of a skimmer?

Rick Clayburgh: You can buy them on line.

Rep D Ruby: The penalties are the use of it a Class B then the subsequent is Class A felony. Should it be more in proportion of what they have stolen?

Rick Clayburgh: There is someone here who can go into detail about that.

Parrell Grossman~Directyor-Consumer Protection & Antitrust Division-Officer of Attorney General: Attachment 1.

11:35

Chairman Keiser: What is the repeal in section 4?

Parrell Grossman: It had a different variation in recoding. It's a lesser version than what we are offering.

Vice Chairman Lefor: Section 3, page 4, lines 6-8, that part makes no sense to me. Why wouldn't we strike that language?

Parrell Grossman: It was intended for a business that legitimately uses a skimmer and is not charge with the crime or possession.

Vice Chairman Lefor: In what circumstances would it be legal?

Parrell Grossman: I would have to look at that further.

Vice Chairman Lefor: I would like more information on that.

Parrell Grossman: We are not opposed to removing that effect.

Vice Chairman Lefor: If there is some legitimate reason, I have no problem with that.

Parrell Grossman: I think that may have come from existing law.

Rep Kasper: This appears to me that it conflicts with line 6 on page 4. It implies that a skimmer can be used but now without the permission of the person. Then on line 11, if you own a skimmer, it's a class A misdemeanor. How would those two work? Page 2, starting on lines 8, does this part of our code state or any other place in code, state & imply that this personal identifying information is the property right & owned by the person?

Parrell Grossman: The first question, is only illegal for that purpose. Second question, that things that are used in a harmful way. I don't know if it's property rights or not.

Rep Kasper: Isn't that something that's important. There is a crime being committed but the property is owned.

Parrell Grossman: That a policy decision.

Rep Kasper: These are unique identifiers to that individual.

Parrell Grossman: I would agree with that about unique identifiers.

Rep D Ruby: What about repealing that & putting in new language rather than making some changes & improvements. What is this doing that slight besides slight definitions changes. Why don't we update the language?

Parrell Grossman: I talked with legislative management & it would be easier

Rep D Ruby: My clarification, it's already illegal, we just need to update the skimming?

Parrell Grossman: I would agree with that.

Rep Richter: Can you explain the drive by?

Parrell Grossman: Someone can access your information with the correct equipment, capture information that is being transmitted & they can scan that information.

Chairman Keiser: There is technology by just standing by the person.

Rep Louser: The square readers, they are misdemeanors, I have one in possession & I'm worried about that. Is it considered a skimming devise?

Parrell Grossman: I would have to look at that but I don't think it would fall under that. It's not used for unauthorized transactions & it's a legitimate devise.

Rep Louser: We referenced of the standing devise, the magnetic strip on a state driver's license or state issued identification card?

Parrell Grossman: I don't have the answer to that question.

Rep Laning: The small square on credit card, are they effective from scanning?

Parrell Grossman: I heard that they can somewhat be effective.

Chairman Keiser: Seems that gas stations have skimming devices that are legal because I'm giving them authority to do it. The issue here isn't whether it's a skimming device that in there but whether it's the use of the information by a skimming device. Isn't that the issue?

Parrell Grossman: That's correct. The definitions are quite broad, on purpose.

Chairman Keiser: It's the illegal use of the information.

Parrell Grossman: That's right. If there is permission.

Mike Rud ~ President-ND Retail & Petroleum Marketer Association: Attachment 2.

31:50

Rep Adams: How do they get into the gas pump?

Mike Rud: Back in the early days, there was only one key to open the pumps, now they have different sets of keys.

Rep D Ruby: Does the money go to the individual & the merchant or do they just get the number & run it up?

Mike Rep D Ruby: In most of the cases, they just use the information by creating a new card?

Rep D Ruby: Does the merchant get their payments so they don't know anything?

Mike Rud: Yes.

Barry Haugen~President of the Independent Community Banks of ND (ICBND's): Attachment 3.

37:45

Rep D Ruby: We already have the law in place, technically already. You don't expect anything substantial or profound if this is passed.

Barry Haugen: You're right but there is more teeth in the possession of these.

Chairman Keiser: This bill could help but we would like to find another solution & achieve something.

Barry Haugen: The is not at the state level but US is behind compared to Europe in protection.

Jeff Olson~Credit Union Association of the Dakotas: We too are in support of this. The reading of chips, the tap & go, we are seeing more of this. We are constantly trying to keep up but the small mom & pop can't keep up. With this bill it's a start & there is more teeth in it.

Rep C Johnson: The credit cards with the chips, are they more secure?

Jeff Olson: Yes, they are supposed to be more secure.

Chairman Keiser: In Taiwan & China, 80% of all transaction are non-cash, non-credit card, it's through their phones. I don't know why phone technology is working but maybe we need to imporve.

Chairman Keiser: Anyone else here to testify on SB 2262, support, opposition, neutral?

Rep Louser: Do you think it be beneficial if we do the skimming for lawful or illegal purposes?

Parrell Grossman: Again, they have to use that device without the authorization of using the information.

Rep Louser: We are primarily focusing the skimming device which is used for theft. If we defined a scanning device that is used business transaction & used without the authorization, then fraud or theft applies anyway. My concern we are focusing on the device. The difference between scanner & skimmer. The skimming is illegal. Can we focus on defining the skimmer as the problem & have the possession of the skimmer a misdemeanor?

Parrell Grossman: The crime still needs to use that device to skim. If that's the concern of the committee, we can change it.

Rep D Ruby: We take a lot of credit card payments over the phone & still do. We were told by a company because we don't have a signature, if they would challenge it, you would have

to return it. There is no way to sign on a bill. If we did the transaction, they came back & said that we used the card, are we illegal in that situation? Would we be subjected to any of these penalties because we ran a card without any signing?

Parrell Grossman: No, I can't see that it's an unauthorized use.

Rep D Ruby: We don't have proof to run the card.

Parrell Grossman: No, I don't see any circumstances that you can be charged.

Chairman Keiser: Anyone else here to testify on SB 2262? Closes the hearing. What are the wishes of the committee?

Rep Adams: Moves for a Do Pass.

Rep Laning: Second.

Chairman Keiser: Further discussion?

Chairman Keiser: I understand the concern raised by Rep Louser, but I think the bill addresses it.

Rick Clayburgh: A skimmer is a specific device that goes over the top of a scanning device.

Chairman Keiser: It doesn't say that but if you read the definition.

Rick Clayburgh: The industry norm, that is how it's interpreted & defined.

Chairman Keiser: The key is the illegal access of information.

Rick Clayburgh: We need the scanning in there as well.

Roll call was taken on SB 2262 for a Do Pass with 9 yes, 2 no, 3 absent & Rep Richter is the carrier.

Date: Mar 6, 2019

Roll Call Vote #: 1

2019 HOUSE STANDING COMMITTEE
ROLL CALL VOTES

BILL/RESOLUTION NO. SB 2262

House Industry, Business and Labor **Committee**

☐ **Subcommittee**

Amendment LC# or Description:

Recommendation

☐ Adopt Amendment
☒ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☐ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions ☐ Reconsider ☐

Motion Made by Rep Adams **Seconded By** Rep Laning

Representatives	Yes	No	Representatives	Yes	No
Chairman Keiser	X		Rep O'Brien	~~Ab~~	
Vice Chairman Lefor	X		Rep Richter	X	
Rep Bosch	~~Ab~~		Rep D Ruby	X	
Rep C Johnson	X		Rep Schauer		X
Rep Kasper	X		Rep Adams	X	
Rep Laning	X		Rep P Anderson	X	
Rep Louser		X	Rep M Nelson	~~Ab~~	

Total (Yes) 9 No 2

Absent 3

Floor Assignment Rep Richter

REPORT OF STANDING COMMITTEE

SB 2262: Industry, Business and Labor Committee (Rep. Keiser, Chairman) recommends **DO PASS** (9 YEAS, 2 NAYS, 3 ABSENT AND NOT VOTING). SB 2262 was placed on the Fourteenth order on the calendar.

2019 TESTIMONY

SB 2262

SENATE INDUSTRY, BUSINESS AND LABOR COMMITTEE
JERRY KLEIN, CHAIRMAN
JANUARY 23, 2019

TESTIMONY BY
PARRELL D. GROSSMAN
DIRECTOR, CONSUMER PROTECTION AND ANTITRUST DIVISION
OFFICE OF ATTORNEY GENERAL
IN SUPPORT OF
SENATE BILL NO. 2262

Mr. Chairman and members of the Senate Industry, Business and Labor Committee. I am Parrell Grossman, and it is my privilege to be the Director of the Attorney General's Consumer Protection and Antitrust Division. I appear on behalf of the Attorney General in support of Senate Bill 2262.

The Attorney General drafted this legislation at the request of the North Dakota Bankers Association and the North Dakota Retailers and Petroleum Marketers Associations. These organizations contacted the Attorney General with an interest in enhancing legislation in the area of scanning or skimming payment cards.

As you are aware devices that capture payment card information often are attached over existing scanning devices on bank ATMs and gas station pumps, etc. Often these ATMs or gas pumps might be in remote locations or out of the owner's line-of-sight, or other locations that might present such opportunities. The consumer thinks they are swiping their cards in a legitimate device that has been placed in a seemingly realistic manner over the actual legitimate device.

In addition to these fixed location scanners, these devices also may be used in retail locations, restaurants, bars, etc. It is quite easy for a perpetrator to use one of these hand-held devices to swipe a card on the merchant's actual payment card processor and make a duplicate swipe on the hand-held device. Many consumers over the years have reported that their payment cards were compromised after visiting various merchants during travel, although this conduct can occur anywhere at any time. This event could happen in any location during times in which the person holding the payment card is temporarily out-of-sight when processing the payment.

Also, there are scanners, whether radio-controlled or otherwise, that can capture payment card information, without the awareness of the cardholders.

This captured information from payment cards is a source of financial and other harm to the card owners and card issuers and can be used to make unauthorized purchases, or it can be sold as a valuable commodity.

There is existing law in NDCC section 12.1-23-17 that makes the use of these devices illegal. However, there really is not a legitimate reason to possess one of these devices

and North Dakota law currently does not make the possession of these devices illegal. It should be and we would like the Legislature to address and fix this problem. Section 3 of this Bill makes it a class A misdemeanor to possess one of these devices with the intent to commit, aid, or abet any unlawful activity.

In looking at our current law on the use of these devices, we reviewed many other states' statutes that make scanning and skimming illegal. We believe our current statute, a good law adopted in 2013, could be significantly improved in some aspects. Because of the current structure of our statute, and the number of changes, it frankly was much easier to suggest the repeal of section 12.1-23-17 (copy attached) and create new law with the proposed changes.

In addition to adding the possession crime, I will highlight some of the other changes. The changes broaden the applicability to computer chips throughout re-encoders, scanning devises and skimmers and now would include capturing information from driver's licenses or state issued identification cards.

The changes create a new definition of a skimming device and make both the use and possession of the skimmer a crime, as opposed to the current structure trying to encapsulate the conduct of using a scanning or re-encoder device within an undefined concept of "skimming." The skimming device in this legislation is more broadly defined to add photographic or visual imaging to other methods of capturing, storing, etc. the financial information contained in a payment card or encoded on a computer chip or magnetic strip.

A scanning device would relate to capturing any type of information on a payment card, driver's license, or any other electronic medium that would allow an authorized (or in this instance "an unauthorized") transaction to occur, or any other unauthorized use of the captured information. It would include radio frequency drive-by capturing of information without the use of a physical device that uses the payment card.

We have incorporated the existing penalties of a class B felony for a first offense and class A felony for a second offense, and added the class A misdemeanor penalties for possession of the devices.

The Attorney General believes these legislative changes will provide a more robust and all-encompassing approach to both the use and possession of these various devices.

I would like to try and briefly address Section 2 of this Bill and the proposed changes regarding the unauthorized use of personal identifying information. The concept of "personal identifying information" is not static and necessarily is ever evolving due to the new and different types of personal information that can and will be used to steal our identities or monies. As a result, the Attorney General would like to propose some new components as set forth in suggested amendments on Page 3, lines 1through 4. "An individual's payment card information" is broader than the existing component of "an

individual's financial institution account number, credit card number, or debit card number" as provided in current law on Page 2, lines 20 through 21.

It is appropriate to add "an individual's biometric data" to the laundry list. "Biometric data" refers to records used to uniquely identify persons, such as fingerprints or retinal scans. Additionally, we propose to add the all-encompassing phrase of "any other numbers, documents, or information that can be used to access another person's financial records." These additional components will definitely broaden the protections for our personal identifying information and provide for appropriate criminal prosecution.

Finally, on Page 3, lines 5 through 6, the Attorney General is offering a significant and long overdue change in existing law. The current law only prohibits the use or attempted use of personal identifying information. While making the proposed changes to the payment card skimming laws, it occurred to the Attorney General that, in addition to the use of such information without authorization or consent, it should be illegal to "obtain or attempt to obtain, transfer, or record" any personal identifying information. The confidential and financial information stored on various payment cards, etc. is scanned or skimmed without permission for the sole purposes of stealing our financial resources or identities. If any of this same information also is "personal identifying information," it also should be illegal and a crime under section 12.1-23 to obtain or transfer this personal identifying information" without authorization or consent of the other individual. However, the Attorney General recognizes this is a policy decision for this Committee and the Legislature.

The Attorney General respectfully recommends that the Senate Industry, Business & Labor Committee give Senate Bill 2262 a "Do Pass" recommendation.

Thank you for your time and consideration. I would be pleased to try and answer any questions.

transaction records that may be preserved in digital formats to represent the true or manipulated transaction data or reports in the electronic cash register and is intended to falsify the electronic records of an electronic cash register or other point-of-sale system.

d. "Transaction data" means items purchased by a customer, the price for each item, a taxability determination for each item, a segregated tax amount for each of the taxed items, the amount of cash or credit tendered, the net amount returned to the customer in change, the date and time of purchase, the name, address, and identification number of the vendor, and the receipt or invoice number of the transaction.

e. "Transaction report" means a report documenting sales, the tax collected, methods of payment, voided sales, or other information at an electronic cash register which is printed on cash register tape at the end of a day or shift, or a report documenting every transaction at an electronic cash register that is stored electronically.

2. It is unlawful to willfully sell, purchase, possess, install, transfer, manufacture, own, or use in this state, an automated sales suppression device, zapper, or phantom-ware.

3. Any person convicted of a violation under subsection 2 is guilty of a class B felony. Any person convicted of a second or subsequent violation of subsection 2 is guilty of a class A felony and also is subject to a civil penalty of not more than one hundred thousand dollars.

4. It is a defense to prosecution under this section that the person purchased, possessed, installed, transferred, owned, or used in this state, an automated sales suppression device, zapper, or phantom-ware for a legitimate purpose.

5. Any person violating subsection 2 is liable for all sales and use tax, income tax, or other tax under title 57, and any county or city sales and use tax imposed under sections 11-09.2-05 and 40-05.1-06, and associated penalties and interest due the state as the result of the fraudulent use of an automated sales suppression device, zapper, or phantom-ware. Any tax found to be due must be assessed at double the amount so determined.

6. The person shall forfeit all proceeds associated with the sale or use of an automated sales suppression device, zapper, or phantom-ware. The proceeds forfeited under this section must be deposited with the state treasurer for deposit in the state general fund.

7. An automated sales suppression device, zapper, or phantom-ware, and the cash register or other device containing the device or the software, is contraband and subject to forfeiture in accordance with chapter 29-31.1.

12.1-23-17. Unlawful skimming of credit, debit, or other electronic payment cards - Penalty.

1. For purposes of this section:

a. "Authorized card user" means any person with the empowerment, permission, or competence to use an electronic payment card.

b. "Electronic payment card" means a credit card, charge card, debit card, hotel key card, stored value card, or any other card that is issued to an authorized card user which allows the user to obtain, purchase, or receive goods, services, money, or anything else of value from a merchant.

c. "Merchant" means an owner or operator of a retail mercantile establishment or an agent, employee, lessee, consignee, officer, director, franchisee, or independent contractor of a retail mercantile establishment who receives from an authorized user or someone believed to be an authorized user, an electronic payment card or information from an electronic payment card, or what is believed to be an electronic payment card or information from an electronic payment card, as the instrument for obtaining, purchasing, or receiving goods, services, money, or anything else of value from the retail mercantile establishment.

d. "Re-encoder" means an electronic device that places encoded information from the magnetic strip or stripe of an electronic payment card onto the magnetic strip or stripe of a different electronic payment card.

e. "Scanning device" means a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of an electronic payment card.

2. A person is guilty of unlawful skimming if the person uses:
   a. A scanning device to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of an electronic payment card without the permission of the authorized user of the electronic payment card, with the intent to defraud the authorized user of the electronic payment card, the issuer of the electronic payment card, or a merchant; or
   b. A re-encoder to place information encoded on the magnetic strip or stripe of an electronic payment card onto the magnetic strip or stripe of a different electronic payment card without the permission of the authorized user of the card from which the information is being re-encoded, with the intent to defraud the authorized user of the electronic payment card, the issuer of the electronic payment card, or a merchant.
3. Any person convicted of a violation under subsection 2 is guilty of a class B felony. Any person convicted of a second or subsequent violation of subsection 2 is guilty of a class A felony and also is subject to a civil penalty of not more than one hundred thousand dollars.

SB2262 1/23/19 Att #2

January 23, 2019

SENATE INDUSTRY, BUSINESS AND LABOR COMMITTEE
SB 2262

Good morning Mr. Chairman and members of the Senate Industry, Business and Labor Committee. For the record, my name is Barry Haugen and I am President of the Independent Community Banks of North Dakota (ICBND). Our membership totals 60 independent community banks throughout our state. In addition, ICBND's for profit sister company - ICB Services - operates a sort of "banker's bank" for nearly 50 participating banks in a bank branded credit card program that has over 26,000 credit cards issued with an annual spend of about $110 million. So our organization and its members certainly know payment card fraud as almost all of those members issue credit cards and debit cards. And if you issue cards, you have fraud. Simple as that.

As such, we stand in strong support of Senate Bill 2262 and recommend that the committee give this bill a do pass recommendation. It provides to modernize code and puts additional teeth into the law to prosecute those who are caught possessing and/or using skimmers, or re-encoders or scanning devices to unlawfully obtain payment card information.

We typically think of the "pay at the pump" scenario when we discuss this type of fraud because it is very prevalent, there are many other vulnerable points of our commerce system that are affected as well by these white collar criminals.

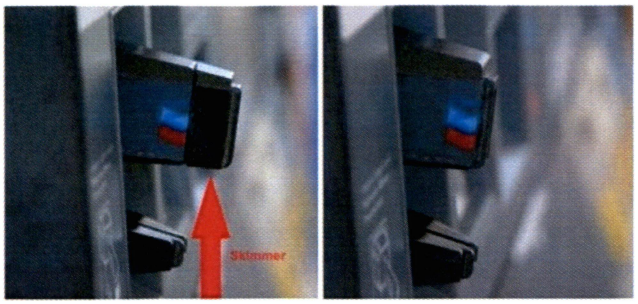
- ATM Skimming is huge and recently occurred with one of our members to a machine in the entry way of their bank.
- Skimmers at restaurants that easily fit in the palm of a hand and can read the necessary data.
- Self -Checkouts such as you see in grocery stores and especially Walmart.
- The trend of transactions without personal interaction will certainly grow and that's a particularly susceptible situation.

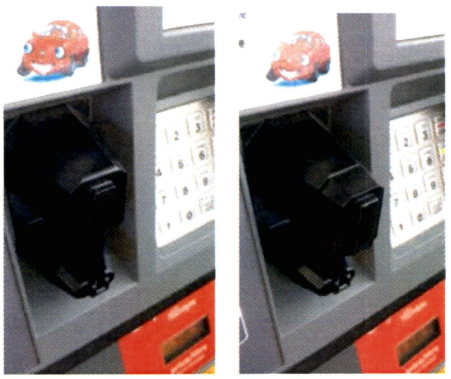
So what happens once the fraud is discovered? Well, obviously there's the financial loss potential. Beyond that, once a card is defrauded and the issuing bank learns of that fraud, generally the card is cancelled and then reissued incurring the costs of the plastic and more importantly staff time and of course the incredible inconvenience to the customer of having to wait at least three business days for a new card and changing any autopay arrangements such as Amazon or Netflix. We've all likely experienced this.

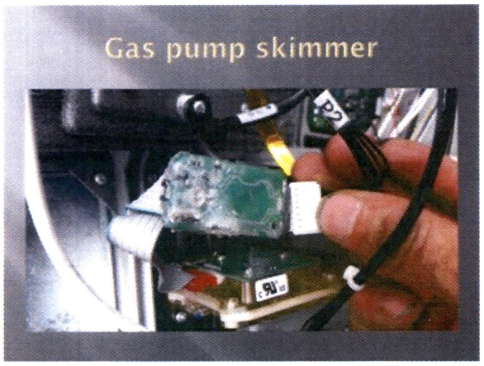
We know this bill isn't going to eliminate card payment fraud or keep the bad guys up at night, but it's better than what we have and ask for a "do pass" recommendation to Senate Bill 2262.

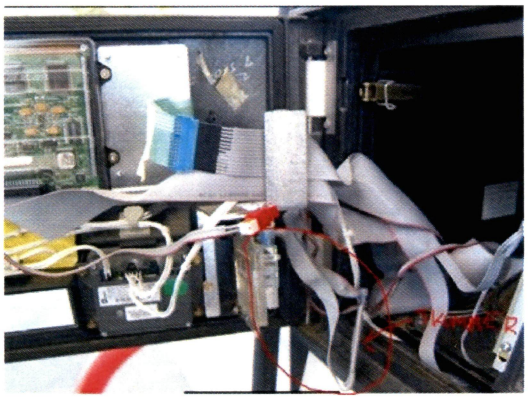
SB2262 1/23/19 Att#3

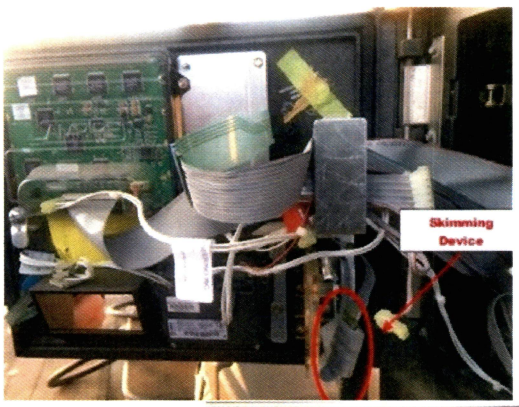
Credit Card Skimmers & Security Seal

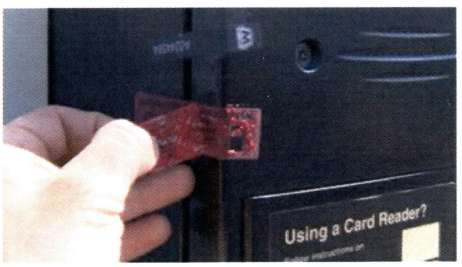


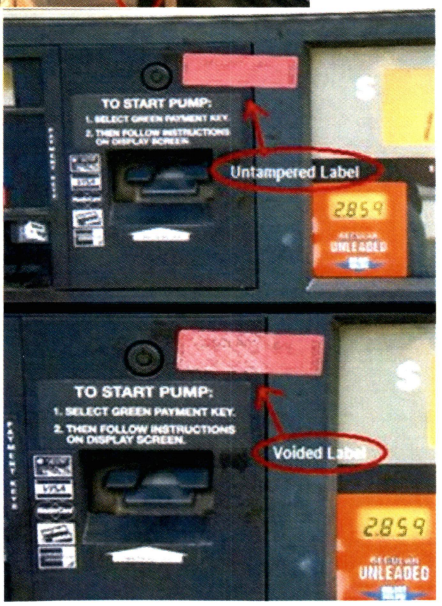












Attachment 1

HOUSE INDUSTRY, BUSINESS AND LABOR COMMITTEE
GEORGE KEISER, CHAIRMAN
MARCH 6, 2019

TESTIMONY BY
PARRELL D. GROSSMAN
DIRECTOR, CONSUMER PROTECTION AND ANTITRUST DIVISION
OFFICE OF ATTORNEY GENERAL
IN SUPPORT OF
SENATE BILL NO. 2262

Mr. Chairman and members of the House Industry, Business and Labor Committee. I am Parrell Grossman, and it is my privilege to be the Director of the Attorney General's Consumer Protection and Antitrust Division. I appear on behalf of the Attorney General in support of Senate Bill 2262.

The Attorney General drafted this legislation at the request of the North Dakota Bankers Association and the North Dakota Retailers and Petroleum Marketers Associations. These organizations contacted the Attorney General with an interest in enhancing legislation in the area of scanning or skimming payment cards.

As you are aware devices that capture payment card information often are attached over existing scanning devices on bank ATMs and gas station pumps, etc. Often these ATMs or gas pumps might be in remote locations or out of the owner's line-of-sight, or other locations that might present such opportunities. The consumer thinks they are swiping their cards in a legitimate device that has been placed in a seemingly realistic manner over the actual legitimate device.

In addition to these fixed location scanners, these devices also may be used in retail locations, restaurants, bars, etc. It is quite easy for a perpetrator to use one of these hand-held devices to swipe a card on the merchant's actual payment card processor and make a duplicate swipe on the hand-held device. Many consumers over the years have reported that their payment cards were compromised after visiting various merchants during travel, although this conduct can occur anywhere at any time. This event could happen in any location during times in which the person holding the payment card is temporarily out-of-sight when processing the payment.

Also, there are scanners, whether radio-controlled or otherwise, that can capture payment card information, without the awareness of the cardholders.

This captured information from payment cards is a source of financial and other harm to the card owners and card issuers and can be used to make unauthorized purchases, or it can be sold as a valuable commodity.

There is existing law in NDCC section 12.1-23-17 that makes the use of these devices illegal. However, there really is not a legitimate reason to possess one of these devices

and North Dakota law currently does not make the possession of these devices illegal. It should be and we would like the Legislature to address and fix this problem. Section 3 of this Bill makes it a class A misdemeanor to possess one of these devices with the intent to commit, aid, or abet any unlawful activity.

In looking at our current law on the use of these devices, we reviewed many other states' statutes that make scanning and skimming illegal. We believe our current statute, a good law adopted in 2013, could be significantly improved in some aspects. Because of the current structure of our statute, and the number of changes, it frankly was much easier to suggest the repeal of section 12.1-23-17 (copy attached) and create new law with the proposed changes.

In addition to adding the possession crime, I will highlight some of the other changes. The changes broaden the applicability to computer chips throughout re-encoders, scanning devises and skimmers and now would include capturing information from driver's licenses or state issued identification cards.

The changes create a new definition of a skimming device and make both the use and possession of the skimmer a crime, as opposed to the current structure trying to encapsulate the conduct of using a scanning or re-encoder device within an undefined concept of "skimming." The skimming device in this legislation is more broadly defined to add photographic or visual imaging to other methods of capturing, storing, etc. the financial information contained in a payment card or encoded on a computer chip or magnetic strip.

A scanning device would relate to capturing any type of information on a payment card, driver's license, or any other electronic medium that would allow an authorized (or in this instance "an unauthorized") transaction to occur, or any other unauthorized use of the captured information. It would include radio frequency drive-by capturing of information without the use of a physical device that uses the payment card.

We have incorporated the existing penalties of a class B felony for a first offense and class A felony for a second offense, and added the class A misdemeanor penalties for possession of the devices.

The Attorney General believes these legislative changes will provide a more robust and all-encompassing approach to both the use and possession of these various devices.

I would like to try and briefly address Section 2 of this Bill and the proposed changes regarding the unauthorized use of personal identifying information. The concept of "personal identifying information" is not static and necessarily is ever evolving due to the new and different types of personal information that can and will be used to steal our identities or monies. As a result, the Attorney General would like to propose some new components as set forth in suggested amendments on Page 3, lines 1through 4. "An individual's payment card information" is broader than the existing component of "an

SB 2262

Attachment 1
Mar 6, 2019

individual's financial institution account number, credit card number, or debit card number" as provided in current law on Page 2, lines 20 through 21.

It is appropriate to add "an individual's biometric data" to the laundry list. "Biometric data" refers to records used to uniquely identify persons, such as fingerprints or retinal scans. Additionally, we propose to add the all-encompassing phrase of "any other numbers, documents, or information that can be used to access another person's financial records." These additional components will definitely broaden the protections for our personal identifying information and provide for appropriate criminal prosecution.

Finally, on Page 3, lines 5 through 6, the Attorney General is offering a significant and long overdue change in existing law. The current law only prohibits the use or attempted use of personal identifying information. While making the proposed changes to the payment card skimming laws, it occurred to the Attorney General that, in addition to the use of such information without authorization or consent, it should be illegal to "obtain or attempt to obtain, transfer, or record" any personal identifying information. The confidential and financial information stored on various payment cards, etc. is scanned or skimmed without permission for the sole purposes of stealing our financial resources or identities. If any of this same information also is "personal identifying information," it also should be illegal and a crime under section 12.1-23 to obtain or transfer this personal identifying information" without authorization or consent of the other individual. However, the Attorney General recognizes this is a policy decision for this Committee and the Legislature.

The Attorney General respectfully recommends that the House Industry, Business & Labor Committee give Senate Bill 2262 a "Do Pass" recommendation.

Thank you for your time and consideration. I would be pleased to try and answer any questions.

Attachment 2

Testimony SB 2262

March 6, 2019- House IBL Committee

Chairman Keiser and members of the House IBL Committee:

For the record, my name is Mike Rud. I serve as president of the North Dakota Retail and Petroleum Marketers Association. On behalf of well over 1,000 business outlets our joint associations represent across the state, we urge a DO PASS recommendation on SB 2262.

One of the more successful tools of 21st century crooks is the skimmer. Thieves attach them to ATMs, gas pumps and other places people swipe their credit and debit cards. The thieves use this information to clone your card, and once they have a clone, they can drain your bank account, or run up huge bills and trash your credit before you even know it.

Several years ago, four men were arrested for allegedly stealing $2.1 million using skimmers at gas stations across the Southern United States. With an average gas transaction of $50, those thieves needed to skim approximately 42,000 transactions of people buying gas. These skimmers were hidden inside the pumps. The skimmers were equipped with Bluetooth so the thieves could drive by and extract the collected numbers and PINs wirelessly.

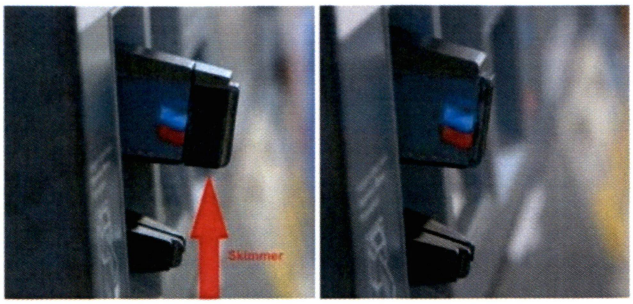
NDPMA and NDRA believe SB 2262 brings much needed stiffer penalties to those found in possession and/or using the credit card skimming devices. We ask for a DO PASS recommendation on SB 2262.

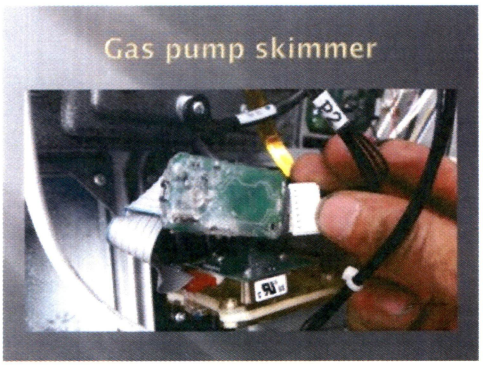
1014 East Central Avenue • PO Box 1956 • Bismarck, ND 58502 • 701-223-3370 • Fax 701-223-5004
Web Address: ndretail.org • ndpetroleum.org

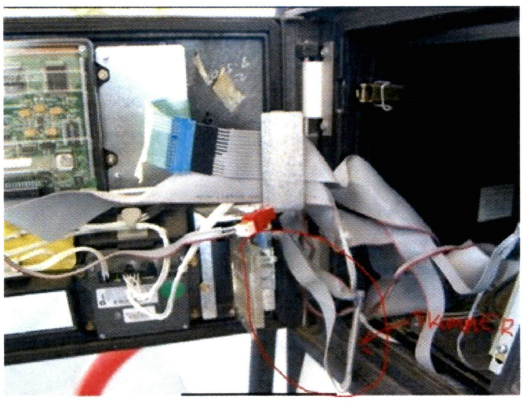
SB 2262

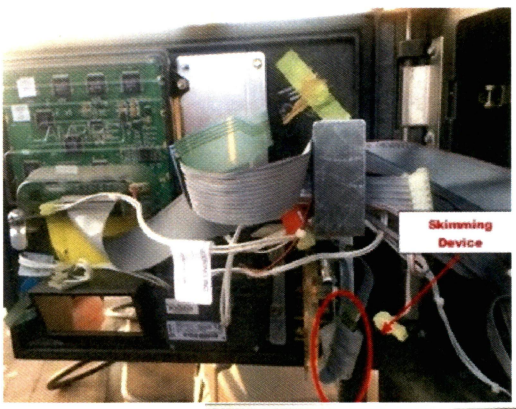
Attachment 2
Mar 6, 2019

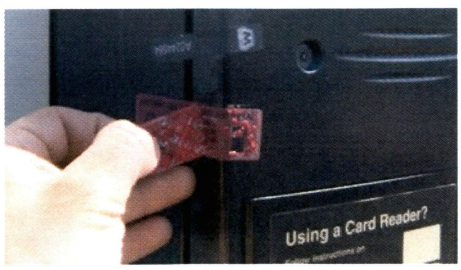
Credit Card Skimmers & Security Seal

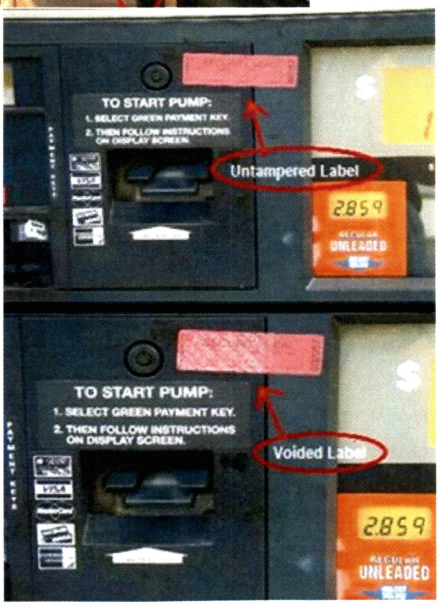












Attachment 3

March 6, 2019

HOUSE INDUSTRY, BUSINESS AND LABOR COMMITTEE
SB 2262

Good morning Mr. Chairman and members of the House Industry, Business and Labor Committee. For the record, my name is Barry Haugen and I am President of the Independent Community Banks of North Dakota (ICBND). Our membership totals 60 independent community banks throughout our state. In addition, ICBND's for profit sister company - ICB Services - operates a sort of "banker's bank" for nearly 50 participating banks in a bank branded credit card program that has over 26,000 credit cards issued with an annual spend of about $110 million. So our organization and its members certainly know payment card fraud as almost all of those members issue credit cards and debit cards. And if you issue cards, you get to experience fraud. Simple as that.

As such, we stand in strong support of Senate Bill 2262 and recommend that the committee give this bill a do pass recommendation. It provides to modernize code and puts additional teeth into the law to prosecute those who are caught possessing and/or using skimmers, or re-encoders or scanning devices to unlawfully obtain payment card information.

We typically think of the "pay at the pump" scenario when we discuss this type of fraud because it is very prevalent. There are however many other vulnerable points of our commerce system that are affected as well by these white collar criminals.

- ATM Skimming is huge and recently occurred with one of our members to a machine in the entry way of their bank.
- Skimmers at restaurants that easily fit in the palm of a hand and can read the necessary data.
- Self -Checkouts such as you see in grocery stores and the big box stores.
- The trend of transactions without personal interaction will certainly grow and that's a particularly susceptible situation.

So what happens once the fraud is discovered? Well, obviously there's the financial loss potential. Beyond that, once a card is defrauded and the issuing bank learns of that fraud, generally the card is cancelled and then reissued incurring the costs of the plastic and more importantly staff time and of course the incredible inconvenience to the customer of having to wait at least three business days for a new card and changing any autopay arrangements such as Amazon or Netflix. We've all likely experienced this.

We know this bill isn't going to eliminate card payment fraud or keep the bad guys up at night, but it's better than what we have and respectfully ask for a "do pass" recommendation to Senate Bill 2262.