The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Appropriations

BILL:	CS/CS/SB 766
INTRODUCER:	Appropriations Committee; Criminal Justice Committee; and Senator Rodriguez
SUBJECT:	Payment Card Offenses
DATE:	April 25, 2017 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Erickson	Hrdlicka	CJ	**Fav/CS**
2.	Harkness	Sadberry	ACJ	**Recommend: Fav/CS**
3.	Harkness	Hansen	AP	**Fav/CS**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/SB 766 addresses the unlawful practice of "skimming" (fraudulently obtaining private information from someone's payment card). Specifically, the bill:

- Modifies the offense of fraudulent use of a scanning device to also punish fraudulent use of a skimming device, and specifies that information unlawfully accessed includes information encoded on a computer chip or other storage mechanism of a payment card.
- Modifies the offense of fraudulent use of a reencoder to indicate that the reencoder places information encoded on the computer chip, magnetic strip or stripe, or other storage mechanism of a payment card onto a computer chip, magnetic strip or stripe, or other storage mechanism of a different card.
- Provides that it is a third degree felony to knowingly possess, sell, or deliver a skimming device, provides that this offense does not apply to specified officials, and provides that this offense is also subject to the Florida Contraband Forfeiture Act.

The Criminal Justice Impact Conference (CJIC) estimates the bill will have a "positive insignificant" prison bed impact (an increase of 10 or fewer prison beds). See Section V. Fiscal Impact.

The bill takes effect October 1, 2017.

II. Present Situation:

Skimming

The practice of "skimming" involves obtaining private information from someone's payment card used in an otherwise normal transaction, such as using an ATM.[1] A person engaging in this practice can obtain a victim's card number in different ways, including photocopying receipts, copying a PIN code, or using an electronic scanning device or reencoder to swipe and store a victim's payment card numbers or transfer the data or information to another card.[2] Skimming can occur at a restaurant or bar where the skimmer has possession of the victim's card out of his or her immediate view.[3] Similarly, skimming can also occur at gas stations when a third-party cardreading device is installed either outside or inside a fuel dispenser[4] or other card-swiping terminal.[5]

Florida Law on Unlawful Use of a Scanning Device or Reencoder

Section 817.625(2), F.S., provides that it a crime to use:

- A scanning device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card without the permission of the authorized user of the payment card and with the intent to defraud the authorized user, the issuer of the authorized user's payment card, or a merchant.
- A reencoder to place information encoded on the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card without the permission of the authorized user of the payment card from which the information is being reencoded and with the intent to defraud the authorized user, the issuer of the authorized user's payment card, or a merchant.

---

[1] "Taking a Trip to the ATM?" (July 14, 2011), Federal Bureau of Investigation , *available at* https://www.fbi.gov/news/stories/atm-skimming (last visited on March 24, 2017). *See also Arnauta v. State*, 125 So.3d 1028, 1029 (Fla. 4th DCA 2013) (noting, in part, that charges were filed against the defendant after police discovered that the defendant had used an ATM skimming device to withdraw money from customer accounts and after police searched the defendant's residence, storage units and vehicle, and discovered a multitude of ATM parts, molds, ATM keypads, circuit boards, blank bank credit cards, magnetic strips, and bank card readers/writers).

[2] Feinberg, Ashley, "The Evolution of ATM Skimmers" (August 27, 2014), *Gizmodo*, *available at* http://gizmodo.com/the-terrifying-evolution-of-atm-skimmers-1626794130 (last visited on March 24, 2017).

[3] Denny, Dawn, "Cashier Linked to Credit Card Skimming Scam, Police Say" (May 20, 2014), KXAN, *available at* http://kxan.com/2014/05/20/restaurant-cashier-linked-to-credit-card-skimming-scam-police-say/ (last visited on March 24, 2017).

[4] Jacobson, Susan, "State Finds 103 Credit-Card Skimmers in 3-month Inspection of Gas Pumps" (May 19, 2015), *Orlando Sentinel*, *available at* http://www.orlandosentinel.com/business/os-gas-pump-skimmers-20150519-story.html (last visited on March 24, 2017).

[5] Musil, Steven, "13 Indicted in $2M Gas Station Card-Skimming Scheme" (January 22, 2014), CNET, *available at* https://www.cnet.com/news/13-indicted-in-2m-gas-station-card-skimming-scheme/ (last visited on March 24, 2017).

A first violation of s. 817.625(2), F.S., is a third degree felony;[6] a second or subsequent violation of this subsection is a second-degree felony.[7] A violation of s. 817.625(2), F.S., is also subject to the Florida Contraband Forfeiture Act (ss. 932.07 – 932.7062, F.S.).[8]

Section 817.625, F.S., provides the following definitions of relevant terms:

- "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 a payment card.
- "Reencoder" means an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different payment card.
- "Payment card" means a credit card, charge card, debit card, or any other card that is issued to an authorized card user and that allows the user to obtain, purchase, or receive goods, services, money, or anything else of value from a merchant.
- "Merchant" means a person who receives from an authorized user of a payment card, or someone the person believes to be an authorized user, a payment card or information from a payment card, or what the person believes to be a payment card or information from a payment card, as the instrument for obtaining, purchasing, or receiving goods, services, money, or anything else of value from the person.[9]

III. Effect of Proposed Changes:

Section 1 amends s. 817.625(2)(a)1., F.S., which currently punishes fraudulent use of a scanning device. The bill modifies this offense to also punish fraudulent use of a skimming device. It also specifies that information unlawfully accessed includes information encoded on a computer chip or other storage mechanism of a payment card.

Section 817.625(2)(a)2., F.S., which currently punishes fraudulent use of a reencoder, is modified to indicate that the reencoder places information encoded on a computer chip, magnetic strip or stripe, or other storage mechanism of a payment card onto a computer chip, magnetic strip or stripe, or other storage mechanism of a different card. The current offense does not mention the terms "computer chip" and "other storage mechanism."

As previously noted, a first violation of s. 817.625(2)(a)1., F.S., or s. 817.625(2)(a)2., F.S., is a third degree felony; a second or subsequent violation is a second degree felony. A violation is also subject to the Florida Contraband Forfeiture Act (ss. 932.07 – 932.7062, F.S.).

Section 817.625(2)(c), F.S., is created, which makes it a third degree felony to knowingly possess, sell, or deliver a skimming device. This paragraph does not apply to the following individuals while acting within the scope of their official duties:

- An employee, officer, or agent of:

[6] Section 817.625(2)(a), F.S. A third degree felony is punishable by up to 5 years in state prison, a fine of up to $5,000, or both. Sections 775.082 and 775.083, F.S. This offense is ranked as a Level 4 offense in s. 921.0022(3)(d), F.S., of the Criminal Punishment Code (Code) offense severity ranking chart.
[7] Section 817.625(2)(b), F.S. A second degree felony is punishable by up to 15 years in state prison, a fine of up to $10,000, or both. Sections 775.082 and 775.083, F.S. This offense is ranked as a Level 5 offense in s. 921.0022(3)(e), F.S.
[8] Section 817.625(2)(b), F.S.
[9] Section 817.625(a) – (d), F.S.

  - A law enforcement agency or criminal prosecuting authority for the state or the federal government;
  - The state courts system as defined in s. 25.382, F.S., or the federal court system; or
  - An executive branch agency in this state.
- A financial or retail security investigator employed by a merchant.

A person who commits a violation of paragraph (2)(c) is also subject to the Florida Contraband Forfeiture Act (ss. 932.07 – 932.7062, F.S.).

The bill makes the following changes regarding definitions of relevant terms:
- Expands the current definition of "scanning device" to include information encoded on a computer chip or other storage mechanism, or from another device that directly reads the information from a payment card.
- Expands the current definition of "reencoder" to include information encoded on a computer chip or other storage mechanism.
- Provides that the terms "scanning device" and "reencoder" do not include a skimming device.
- Defines "skimming device" as a self-contained device that:
  - Is designed to read and store in the device's internal memory information encoded on the computer chip, magnetic strip or stripe, or other storage mechanism of a payment card or from another device that directly reads the information from a payment card; and
  - Is incapable of processing the payment card information stored for the purpose of obtaining, purchasing, or receiving goods, services, money, or anything else of value from a merchant.

Section 2 amends s. 921.0022, F.S., the Criminal Punishment Code offense severity ranking chart, to rank the new skimming device offense (s. 817.625(2)(c), F.S.) in Level 4. The bill also makes technical conforming changes to the description of s. 817.625(2)(a), F.S., in the chart.

Section 3 provides that the bill takes effect October 1, 2017.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The Criminal Justice Impact Conference (CJIC) met on March 2, 2017 and determined the bill will have a "positive insignificant" prison bed impact (an increase of 10 or fewer prison beds).[10]

VI. Technical Deficiencies:

None

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 817.625 and 921.0022.

IX. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS/CS by Appropriations on April 25, 2017:
The committee substitute removes specific reference to a subparagraph that refers to payment card information that a skimming device reads and stores on a skimming device.

CS by Criminal Justice on April 3, 2017:
The committee substitute:

- Modifies the offense of fraudulent use a scanning device to also punish fraudulent use of a skimming device, and specifies that information unlawfully accessed includes information encoded on a computer chip or other storage mechanism of a payment card.
- Modifies the offense of fraudulent use of a reencoder to indicate that the reencoder places information encoded on a computer chip, magnetic strip or stripe, or other

[10] Office of Economic and Demographic Research, The Florida Legislature, *Criminal Justice Impact Conference, SB 766* (Mar. 2, 2017).

storage mechanism of a payment card onto the computer chip, magnetic strip or stripe, or other storage mechanism of a different card.

- Provides that it is a third degree felony to knowingly possess, sell, or deliver a skimming device, provides that this offense does not apply to specified officials, provides that this offense is also subject to the Florida Contraband Forfeiture Act, and ranks this offense in Level 4 of the Code offense severity ranking chart.
- Modifies the current definitions of "scanning device" and "reencoder" and defines "skimming device."

B. Amendments:

None.

This Senate Bill Analysis does not reflect the intent or official position of the bill's introducer or the Florida Senate.