SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

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

BILL: CS/SB 1482

SPONSOR: Criminal Justice Committee and Senator Crist

SUBJECT: Hotel Key Card/Counterfeit

DATE: March 10, 2004 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Erickson	Cannon	CJ	Fav/CS
2.			BI	
3.			ACJ	
4.			AP	
5.				
6.				

I. Summary:

Committee Substitute for Senate Bill 1482 makes it unlawful for any person knowingly to obtain or attempt to obtain credit, or to purchase or attempt to purchase any goods, property, or service, by the use of any false, fictitious, counterfeit, or expired hotel key card or other card with a magnetic strip, or by the use of any hotel key card or other card with a magnetic strip without the authority of the person to whom the card was issued, or by the use of any hotel key card or other card with a magnetic strip in any case where the card has been revoked and notice of revocation has been given to the person to whom it was issued. If the value of the property, goods, or services obtained or which are sought to be obtained is $300 or more, the offender commits grand larceny. If the value of the property, goods, or services obtained or which are sought to be obtained is less than $300, the offender commits petit larceny.

This CS adds hotel key cards and other cards with a magnetic strip to the definition of "access device," which is "personal identification information" for the purpose of unlawfully obtaining or using "personal identification information" (commonly known as "identity theft"). Various penalties are provided in current law for identity theft crimes.

This CS also defines the term "different payment card" to include a hotel key card or other card with a magnetic strip for the purpose of using a reencoder to unlawfully place information encoded on the magnetic strip of a payment card onto the magnetic strip of a different payment card. This offense is a third degree felony (or a second degree felony for a second or subsequent violation).

This CS substantially amends ss. 817.481, 817.568, 817.625, and 921.0022, F.S.

II. Present Situation:

Use of a Hotel Key Card by Identity Thieves
A hotel key card is a card with a magnetic strip that when passed through an electronic lock allows entry into the room.

In the April, 2000 edition of *Security Management*, that magazine reported how identity thieves can use hotel key cards to store credit card information:

> It works like this: a thief gets his hands on a supply of key cards, either by having a hotel employee steal a batch or by buying them. The thief then uses a commercially available decoder/encoder to read information off a stolen credit card and transfer it to an innocent-looking hotel key card. Because the new generation of key cards is the same size as credit and debit cards, the key cards can then be used at ATMs and at point-of-sale swipe readers, where store clerks frequently do not watch patrons performing the transactions.
>
> The scam recently came to light in Southern California when police searched the hideouts of Armenian gang members and found a cache of key cards from a specific hotel. According to Larry Hanna, a detective in the Las Vegas Police Department's intelligence unit who works closely with California police, authorities decided to read what was encoded on the cards. They came up with credit, ATM, and debit card numbers, but no room information.
>
> Blair Abbott, a Phoenix-area detective who has been investigating this type of crime, notes that a few key cards found on a suspect will not raise the same suspicion as would several credit cards bearing different names. Having multiple hotel keys is neither illegal nor uncommon.
>
> *****
>
> When the card information is lifted and placed on hotel key cards, it can be used not only at point of sale and at ATMs but also in association with accomplices working at stores, banks, and credit card companies. Worse yet, the victim continues to use his or her credit card and will attest to having it when contacted by the credit card company, which delays detection of the fraud.
>
> Law Enforcement has had to rely on the laziness of criminals to spot the scheme, Abbott says. Carrying several cards from the same hotel arouses suspicion, says Abbott, as does punching holes in cards and attaching them to a key chain.
>
> It is unclear how widespread the scam is, but Hanna points out that it is so well known in Glendale, California, that the police keep a reader at the booking desk to scan all confiscated hotel key cards. Abbott says the ploy is making the rounds in New York and Chicago as well.

> Abbott is confident that the scam is still only in its infancy. While it started out within only a few crime rings, recently "organized crime has gotten into this in a huge way," he says.

In the November/December, 1999 issue of *Canadian Banker*, that magazine reported the comments of a Canadian law enforcement officer who described how a gas station attendant "swipes the card to register your purchase and then swipes it again, most likely through a skimming machine he has sitting underneath the register where you can't see it." "The second swipe captures all the information needed to make a debit purchase, including the numbers on the front of the card and the bank routing number." Later, the attendant "transfers that information to a laptop computer and, using a machine similar to a printer, transfers it to another plastic card – anything from a bus pass to a hotel key card." To obtain the PIN number, the attendant either uses a hidden camera in the ceiling or a wall to capture the numbers the customer punches in, or has another person stand directly behind the customer and observe the customer punching in the numbers.

In its 2001 annual report to the California Legislature, the Criminal Intelligence Bureau of the California Department of Justice (the California Attorney General), reported that "a gas station in Fresno, California was being used to skim credit card information from the magnetic strips on the back of the cards.... A device was attached to skim the information from the card to another card with a magnetic strip, such as a hotel key card. An employee of the gas station was tied to an Armenian organized criminal group involved in credit card theft, extortion, counterfeit and Medi-Cal fraud." *Organized Crime in California/2001 Annual Report to the California Legislature*. Criminal Intelligence Bureau, California Department of Justice.

In January of 2003, the California newspaper, *The Fresno Bee*, reported that a man was sentenced in federal court for bank fraud and the unauthorized use of access devices. The defendant "admitted he stole information through the use of a card skimmer which was able to read information found on the magnetic strip of customers' credit or debit cards." Most of the information was received from a particular gas station. The prosecutor "said station customers were usually told to run credit cards through twice. The first swipe was through a legitimate card reader that debited their account. The second swipe, through a stand-alone device, captured the information on the magnetic strip." The defendant "then would encode the account numbers and other data onto magnetic strips on the back of nonactivated credit cards or onto the back of plastic room keys, the type used by hotels and motels...." "After the account numbers were converted onto magnetic strips" the defendant "would take the counterfeit cards to automated teller machines and use the customers' personal identification numbers to make cash withdrawals." "Credit card theft nets 18 months/Customers at a northwest Fresno service station were victimized in fraud." *The Fresno Bee* (January 15, 2003).

In December of 2002, the Minnesota newspaper, *The Duluth News-Tribune*, reported that outgoing mail was stolen from six persons in rural Douglas County, Minnesota. The newspaper reported information from an investigating officer that "[t]he thieves used the personal information printed on checks intended for bills to create sophisticated fake drivers' licenses and payroll checks in the victims' names...." "The suspects were able to get their photo on a license in someone else's name with a simple computer program. The license mock-up was printed on 'static stick,'' a plastic commonly used for commercial promotions that sticks to windshields."

The thieves then placed 'static stick' on "blank hotel key cards to get a pretty believable license....." "Police Warn of Identity Theft Douglas County: To Stop a Rash of Rural Thefts, Authorities are Asking Residents Not to Put Outgoing Mail in Their Mailboxes." *The Duluth News-Tribune* (December 20, 2002).

In November of 2002, the California journal, *Sacramento Business Journal*, describing investigations by Sacramento County's ID Theft Task Force, stated that "[e]vidence photos from one bust show tools of the fake ID trade: printers, adhesive remover, glue, pens, blank magnetic cards and retail receipts. Electronic door keys used in hotels get encoded with false data for credit-card swipe machines." "Growing ID thefts put retailers at risk." *Sacramento Business Journal* (November 1, 2002).

Reported Unlawful Use in Florida of Hotel Key Cards and Other Cards
Staff contacted FDLE Special Agent Robert W. ("Wayne") Ivey of FDLE's Ft. Pierce Field Office, who is also the Taskforce Coordinator for FDLE's Operation L.E.G.I.T. (Law Enforcement Getting Identity Thieves). According to Agent Ivey, there are generally two types of counterfeit cards encountered by FDLE investigators: "white plastic" cards or "show and go" cards. A "white plastic" card is any card that contains a magnetic strip upon which credit card information or other personal financial information illegally obtained has been downloaded, and which is used at places where the person's use of the card would not be examined, such as the use of the card in an ATM machine or a card reader at a gas pump. A "show and go" card is also a card that contains a magnetic strip upon which credit card information or other personal financial information illegally obtained has been downloaded, but it is passed off before a person examining the card as the card represented on its face. Generally, hotel key cards that contain illegally obtained personal financial information are of the "white plastic" card type. Agent Ivey indicated to staff that agents have encountered hotel key cards that contain on the magnetic strip illegally obtained personal financial information, along with a wide variety of other white plastic cards that contain such information. He noted that hotel clerks and others could use hotel key cards as blanks to store personal financial information, but also noted that blank cards with magnetic strips are easily obtainable at some office supply stores, since the cards are sold for legitimate purposes. Agent Ivey further stated:

> I can tell you that we have worked tons of cases where the data was stored on every type of card imaginable by the person who was manufacturing the illicit cards for actual use. We have recovered counterfeit cards that were manufactured on hotel keys, security gate access keys, security badges, fuel credit cards, cruise line cards, and even Walt Disney tickets. Essentially anything that has a mag stripe can be utilized to hold the required data. Basically these cards can be made to hold whatever information the programmer directs it to.... We recover these types of cards all the time. One more thing that should be considered in this matter is that if someone working at a hotel wants to steal or use someone's credit card information, they have access to that info through a number of different ways. The bottom line is that a mole inside a business is going to sell that information if the price offered for it is right.

Use of Certain Credit Devices to Unlawfully Obtain Goods, Property, or Services
Section 817.481, F.S., proscribes the acts of knowingly obtaining or attempting to obtain credit, or purchasing or attempting to purchase any goods, property, or service, by using any false,

fictitious, counterfeit, or expired credit card, telephone number, credit number, or other credit device, or by using any of the same credit devices without the authority of the person to whom the card, number, or device was issued, or by using any of the same credit devices in any case where the card, number, or device has been revoked and notice of revocation has been given to the person to whom issued. This section also proscribes the acts of avoiding or attempting to avoid or causing another to avoid payment of the lawful charges, in whole or in part, for any telephone or telegraph service or for the transmission of a message, signal, or other communication by telephone or telegraph or over telephone or telegraph facilities by the use of any fraudulent scheme, means, or method, or any mechanical, electric, or electronic device. The penalty for these acts depends on the value of the property goods, or service illegally obtained or illegally sought to be obtained. If the value is $300 or more, the offender commits grand larceny. If the value is less than $300, the offender commits petty larceny.

The former larceny statute "was repealed and superseded in 1977 by the current theft statute, section 812.014. Ch. 77-342, [sec.] 4, Laws of Fla." *Thomas v. State*, 584 So.2d 1022, 1026 (Fla. 1st DCA 1991) (footnote omitted). The offense of "larceny" "now means the statutory offense of 'theft' by virtue of the provision in section 812.012(2)(d) that defines 'obtains or uses' for purposes of theft under section 812.014 to mean '[c]onduct previously known as stealing; *larceny*; purloining; abstracting; embezzlement; misapplication; misappropriation; conversion; or obtaining money or property by false pretenses, fraud, or deception.' (Emphasis added.)" *Id*. *See Daniels v. State*, 570 So.2d 319, 320 (Fla. 2d DCA 1990).

Accordingly, it appears the "grand larceny" is synonymous with "grand theft." The felony degree and offense severity ranking level of grand theft vary with the type or value of property, goods, or services illegally obtained. Similarly, "petit larceny" is synonymous with "petit theft," which, in most cases, is a second degree misdemeanor. The exceptions are the commission of petit theft when the offender has a prior conviction for any theft (a first degree misdemeanor) and commission of petit theft when the offender has two or more prior convictions of any theft (a third degree felony).

Criminal Use of Personal Identification Information

Section 817.568, F.S., proscribes the "criminal use of personal identification information," a number of criminal acts which are popularly referred to as "identity theft" crimes (or "identity fraud" crimes).

The term "personal identification information" refers, in part, to an "access device." An "access device" is any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access, which can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or which can be used to initiate a transfer of funds, other than a transfer originated solely by paper instrument.

Section 817.568, F.S., provides that it is a third degree felony for any person to, willfully and without authorization fraudulently use, or possess with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual's consent. However, it is a second degree felony, with a 3-year mandatory minimum sentence, to

use the personal identification if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $5,000 or more or if the person fraudulently uses the personal identification information of 10 or more individuals without their consent. When the pecuniary benefit is $50,000 or there are 20 or more victims, the offense is a first degree felony with a 5-year mandatory minimum sentence. When the pecuniary benefit is $100,000 or more or there are 30 or more victims, the offense is a first degree felony with a 10-year mandatory minimum sentence.

It is also a first degree misdemeanor to possess or use personal identification information of an individual for the purpose of harassing that individual.

If an offense prohibited under s. 817.568, F.S., was facilitated or furthered by the use of a public record, the offense is reclassified to the next higher degree.

It is also a second degree felony for any person to, willfully and without authorization, fraudulently use personal identification information concerning an individual who is less than 18 years of age without first obtaining the consent of that individual or of his or her legal guardian.

It is also a second degree felony for any person who is in the relationship of parent or legal guardian, or who otherwise exercises custodial authority over an individual who is less than 18 years of age, to willfully and fraudulently use personal identification information of that individual.

Unlawful Use of a Scanning Device or Reencoder
Section 817.625, F.S., proscribes the unlawful use of a scanning device or reencoder. It is a third degree felony (or a second degree felony for a second or subsequent violation) for a person to use a scanning device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip of a payment card, or use a reencoder to place information encoded on that magnetic strip onto the magnetic strip of a different card, without the permission of the authorized user of the card and with the intent to defraud the authorized user, the issuer of the authorized user's card, or a merchant.

A "payment card" is 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.

III. Effect of Proposed Changes:

Provided is a section-by-section analysis of the CS:

Section 1
Section 1 amends s. 817.481, F.S., to make it unlawful for any person knowingly to obtain or attempt to obtain credit, or to purchase or attempt to purchase any goods, property, or service, by the use of any false, fictitious, counterfeit, or expired hotel key card or other card with a magnetic strip, or by the use of any hotel key card or other card with a magnetic strip without the authority of the person to whom the card was issued, or by the use of any hotel key card or other card with a magnetic strip in any case where the card has been revoked and notice of revocation

has been given to the person to whom it was issued. If the value of the property, goods, or services obtained or which are sought to be obtained is $300 or more, the offender commits grand larceny. If the value of the property, goods, or services obtained or which are sought to be obtained is less than $300, the offender commits petit larceny.

It appears that the true or authentic hotel key card or other card with a magnetic strip is a card issued by the issuer that does not allow a person to obtain credit or make purchases. Conversely, the false, fraudulent, or counterfeit card is the card that contains information that was not provided by the issuer upon issuance of the card or by any authorization of the issuer, but which, nevertheless, is on the card and allows the card's user to obtain credit or make purchases. If a person knowingly uses the false or fraudulent card to obtain credit or make purchases, he or she commits the offense.

It appears that the crime of using a hotel key card or other card with a magnetic strip without the authority of the card's authorized user, applies to any use of the card not authorized by the authorized user of the card. By the plain language, criminal liability does not appear to attach to the issuer of the card or to any other person who places but does not use information on the card that the authorized user has not authorized.

It appears that the reference to "revoked" card would be to a card that has been revoked or deactivated by the issuer of the card.

Section 2
Section 2 amends s. 817.568, F.S., to add hotel key cards and other cards with a magnetic strip to the definition of "access device," which is "personal identification information" for the purpose of unlawfully obtaining or using "personal identification information" (commonly known as "identity theft"). Various penalties are provided in current law for identity theft crimes. (See "Present Situation" section of this analysis for a description of the crimes and penalties.)

Criminal liability attaches only to willful and unauthorized fraudulent use of personal identification information, or unauthorized possession of that information with intent to fraudulently use that information.

Section 3
Section 3 amends s. 817.568, F.S., to define the term "different payment card" to include a hotel key card or other card with a magnetic strip for the purpose of using a reencoder to unlawfully place information encoded on the magnetic strip of a payment card onto the magnetic strip of a different payment card. This offense is a third degree felony (or a second degree felony for a second or subsequent violation).

Criminal liability only attaches to use of a reencoder to place information encoded on the magnetic strip of a payment card onto the magnetic strip of a different payment card, without the permission of the authorized user of the card and with the intent to defraud the authorized user, the issuer of the authorized user's card, or a merchant. By its plain language, criminal liability would not attach to the merchant or issuer of the card if the issuer stores information on the card by the use of a reencoder, even information stored without the permission of the authorized user

of the card, unless the merchant or issuer of the card stored the information with intent to defraud the authorized user.

Section 4
Section 4 reenacts ss. 921.0022(3)(b), (d), (e), (h), and (i), F.S. (various severity levels in the Criminal Punishment Code's offense severity ranking chart), to incorporate the amendments made by this act to ss. 817.481, 817.568, and 817.625, F.S., in references thereto.

Section 5
Section 5 provides that the act takes effect July 1, 2004.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The Criminal Justice Impact Conference (CJIC) has not yet met to review and determine if CS/SB 1482 has a prison bed impact. However, the CJIC has estimated that SB 1482 is likely to have an insignificant prison bed impact. The CS does not differ greatly in substance from the original bill.

VI. Technical Deficiencies:

None.

VII. Related Issues:

The problem of identity thieves placing illegally obtained credit card information and other personal financial information on hotel key cards is distinguishable from another issue regarding hotel key cards that received press coverage last year as a result of a widely circulated e-mail. It was reported that hotels were storing personal financial information of guests on hotel key cards.

The storing of personal financial information on hotel key cards was disputed by hotel industry representatives and others. Linda Foley of the Identity Theft Resource Center in Washington, D.C., was reported as stating: "It was an experiment tried in one city, and not for a long time. It was far too costly, and discontinued...." "Key Card Scare tells us to mind ID matters." *The Record* (Hackensack, New Jersey) (November 23, 2003). *See* "Hotel room key rumor checks but it's not true your credit info is embedded in them." *The Charlotte Observer* (NC) (November 17, 2003) (Kathy Shepard, a spokeswoman for Hilton Hotels Corp. in Beverly Hills, California, was reported as stating: "The only thing we include on Hilton key cards is the room number and arrival and departure dates.")

The Charlotte Observer also reported: "[o]ther hotel chains have the same policy, experts say." *See The Record, supra* ("The folks at Doubletree, as well as at other hotel chains, all report that they are not embedding any kind of information in these cards.").

An investigator in the Pasadena Police Department was reported to be the source of the original e-mail regarding hotel key cards. An explanation of the e-mail was issued by that department, which stated: "As of today, detectives have contacted several large hotels and computer companies using plastic card key technology and they assure us that personal information, especially credit card information, is not included on their key cards. The one incident referred to appears to be several years old." *The Record, supra*.

A spokesperson for the Pasadena Police Department did note that a hotel clerk storing personal financial information on a hotel key card could "potentially happen." "Hotels can't erase myth about credit card information on room keys." *Las-Vegas Review Journal* (November 10, 2003). This journal also reported that Tracey Brierly, a deputy attorney general in Nevada's Bureau of Consumer Protection had attended a technology crime conference in which volunteers were asked to provide hotel key cards to a conference speaker. One card brought up a name and partial address and another brought up a name, address, and credit number. *Id.*

The Record reported: "'There are potential risks,' said Greg Meyer, chief technology officer at iJET, an intelligence agency for the travel industry. 'There are very few controls, technological or regulatory.' New technology has, as usual, outpaced the ability to control it, so there are risks concerning privacy, Meyer said. But iJET doesn't see the key card issue as a major problem." Similar comments were reported in *The Charlotte Observer*: "'Hotels do have the capacity to encode virtually anything on a card key,' says online travel columnist Joe Brancatelli. 'But almost none of them put anything more than check-in and check-out times on the cards.'"

Based on these newspaper and journal accounts, it appears that there are no reported instances of hotels currently authorizing the storing of guests' personal financial information on hotel key cards. It is technologically possible to store personal financial information on a hotel key card

and a hotel employee with access to a guest's personal financial information and the guest's hotel key card could store such information on the card, but so could any other person with similar access.

VIII. Amendments:

None.