Approved:February 23, 2004
Date

MINUTES OF THE SENATE FINANCIAL INSTITUTIONS AND INSURANCE COMMITTEE

The meeting was called to order by Chairperson Ruth Teichman at 9:30 a.m. on February 5, 2004 in Room 234-N of the Capitol.

All members were present except:
Senator David Adkins- Absent

Committee staff present:
Bill Wolff, Legislative Research
Ken Wilke, Revisor of Statutes Office
Nancy Shaughnessy, Committee Secretary

Conferees appearing before the committee:
Senator Phil Journey
Joseph P. Zingher
Kansas Banker's Association
Matthew Goddard
K.C.. Blodgett
Ron Gaches

Others attending:
See Attached List.

Senator Teichman introduced Roderick Bremby, Secretary of the Kansas Dept. Of Health and Environment. Secretary Bremby presented an overview (Attachment 1) of the Department and specifically the health care data collection to support health policy development. The outgrowth of data base seeded at KDHE is the development of a database called the KHIS(Kansas Health Insurance Information System).KHIS is a claims database the Commissioner uses to address information mandates, insurance mandates and other health insurance issues.

This information has been used on several occasions to support legislative mandate discussion. KHIS is a model for other states in that it provides cost information, not only claims information. Future goals for enhanced service includes obtaining health utilization data, provider specific data that includes financial information, quality and outcome data. The Governor's office has recently expanded the Board to include 3 (three) additional members, two members would represent business, large and small and the third will be a member at large.

Senator Barnett commented he appreciated hearing the report to the Committee. This kind of data will be critically important in the future as the legislature makes decisions regarding health care issues.

The Chair then opened the hearings on **SB 333-ATM-PIN reverse protection** and introduced the first conferee.
Senator Phil Journey presented his testimony(Attachment 2) and commented it was the first bill he had filed in his brief legislative career. ATM crime is a growing problem and this bill would require in the installation of ATM machines a system which would allow the customer to initiate a distress signal being relayed to local law enforcement agencies. The conferee then introduced a technical witness and inventor of the ATM software to explain it's function.

Mr. Joseph Zingher, owner of the SafetyPIN system testified(Attachment3) as a proponent of the bill. He stated that all an emergency PIN system would require is a new set of instructions being added to software already in place and it would provide enhanced protection of ATM customers. He addressed the primary objections of cost and the problem of the panicky customer.

Chuck Stones of the KBA(Kansas Bankers Association) testified in opposition to the bill.(Attachment 4) He assured the Committee that customer safety was of the utmost concern to the financial institutions that he represents. However, research shows that of all the steps that can be taken to improve customer security, careful attention to the "3L's", location, lighting and landscaping, plus education produce the

best results.The financial institutions are concerned that the measures they take be effective and this particular product does not appear to meet that standard.

Matthew Goddard of the Heartland Community Bankers Association presented testimony in opposition to the bill.(Attachment 5) HCBA and their member institutions are committed are to providing ATM users with a safe banking experience. They are opposed, however, to legislation requiring ATM owners to use a specific and unproven security program.

K.C. Blodgett , Supervisor of Security Personnel, Commerce State Bank presented testimony(Attachment 6) opposing **SB 333.** He stated that in his past experience as a police officer, indicates he does not feel that this is a common crime. His personal belief is that the bill would not be beneficial to anyone, the victim, the financial institution or law enforcement.

Ron Gaches representing bank clients testified before the Committee in opposition to the bill. (Attachment 7) He addressed the significant amount of security measures that his client banks have taken to assure the safety of their customers. The reverse PIN technology mandated in **SB `333** has not been demonstrated to improve the security of ATM users. It is worth noting, that mandates similar to this one has been discussed in several states but adopted by none.

Bill Henry of the Kansas Credit Union Association submitted written testimony in opposition to the bill. (Attachment 8)

The Chair asked the Committee if there were any questions, hearing none, the hearing on **SB 333** was closed.

Meeting adjourned at 10:35 A.M.

The next meeting was scheduled for: Tuesday Feb. 10, 2004

SENATE FINANCIAL INSTITUTIONS & INSURANCE

Date: THURS 2-5-04

Name:	Representing:
Bill Henry	Ks Credit Union Assn
Ron Gaches	Commerce Bank
Chuck Stokes	KBA
Kathy Olsen	"
Dub Iams	"
Larry Carlson	Commerce Bank, Topeka
K.C. Blodgett	"
Joseph P. Zingher	WITNESS
Senator Jay Emler	
Shari Weber	Community Bankers Assn of K

K A N S A S

RODERICK L. BREMBY, SECRETARY

KATHLEEN SEBELIUS, GOVERNOR

DEPARTMENT OF HEALTH AND ENVIRONMENT

Testimony on Vision for Data Collection
to the
Senate Financial Institutions and Insurance Committee

by Roderick L. Bremby

Secretary
Kansas Department of Health and Environment

Chair
Health Care Data Governing Board

February 5, 2004

Mr. Chairman and committee members, thank you for the opportunity to speak today on our data vision and to describe the efforts under way at the Kansas Department of Health and Environment (KDHE) regarding health care data collection to support health policy development. KDHE has the honor and responsibility of being the steward of a number of datasets that are critical to the future of decision-making for the health of Kansans. I'm proud to be able to say that what we have now is information about Kansans' health experiences--from Kansas sources. Before delving into the future of the data, I think it may be useful to provide some background regarding the governing board. Over ten years ago, at a time when health care reform was being hotly debated, then-Secretary of Health and Environment, Dr. Robert Harder, convinced the 1993 Legislature the need to gather information about the health of Kansans. At that time, Kansas had very little data in the public domain about Kansans' health experiences which forced policymakers to make decisions with information extrapolated or interpolated from national estimates. This was considered unacceptable, and with the leadership of then-Senator Sandy Praeger, the Secretary of Health and Environment was charged with developing a health care database.

OFFICE OF THE SECRETARY
CURTIS STATE OFFICE BUILDING, 1000 SW JACKSON ST., STE. 540, TOP
Voice 785-296-0461 Fax 785-368-6368 http://www.kd

Senate F I & I Committee
Meeting Date: FEB 5, 2004
Attachment No.: 1

To advise the Secretary, the Health Care Data Governing Board was created. The structure of this Board included members of the health care provider community that owned much of the data the state would need to assert its role in decision-making processes. This scheme differed from many of the data commission structures in other states where businesses and consumers were at the helm. A list of the current Governing Board membership is attached for your information.

Activities surrounding health care database function within KDHE generated a number of initiatives that have improved the body of health information available to the state and contributed to the efficiency of state government. An outgrowth of the health care database seated at KDHE was the development of a database called the Kansas Health Insurance Information System (KHIIS) to address the health care statistical plan established by the Kansas Insurance Commissioner. KHIIS is a claims database the Commissioner uses to address insurance mandates and other health insurance issues. This database has been used on a number of occasions to support legislative mandate discussions, which are summarized in another attachment.

Under the board's guidance, we were able to obtain and make available health care professional and hospital discharge data. These include reports published and disseminated in hard copy and via the Governing Board's website. Tailored data products are another way information is disseminated from the Health Care database. In 2003 over 213 specialized data requests were fulfilled with more than half of the data requested from businesses, 15% from governmental entities and the remaining 30% from local and educational entities. In addition, over 106,000 successful website hits were recorded through the Information Network of Kansas (INK). Interestingly, information about nurses is the most frequently requested data. Finally, for those customers needing greater access to the database, KDHE has entered into Memoranda of Understanding.

The board's successes notwithstanding, we need to do more to better serve the health needs of Kansans; we need to obtain health utilization data, provider-specific data that includes financial information, quality and outcome data. To that end, I have proposed a reorganization scheme that includes changes to the board structure: the Governor's Office introduced legislation yesterday to

expand the board by three additional members; and I will appoint an executive committee that will focus on the necessary elements required to achieve a useful database that can be used to formulate health policy; and I will devote dedicated staff to provide support for the board. Our vision is increased access to the many sources of data within state agencies and those outside to enhance the ability of policy makers to make informed health and health care decisions.

I'd like to stand for questions at this time.

STATE OF KANSAS

SENATOR PHILLIP B. JOURNEY
STATE SENATOR, 26TH DISTRICT
P.O. BOX 471
HAYSVILLE, KS 67060

STATE CAPITOL
300 S.W. 10TH AVENUE
TOPEKA, KANSAS 66612-1504
(785) 296-7367
E-mail: journey@senate.state.ks.us

TOPEKA

SENATE CHAMBER

COMMITTEE ASSIGNMENTS
MEMBER: ASSESSMENT & TAXATION
NATURAL RESOURCES
PUBLIC HEALTH AND WELFARE

Testimony in Support of Senate Bill 333 Presented by State Senator Phillip B. Journey, 26th District

On February 5th, 2004, before the Senate Financial Institutions and Insurance Committee, the Honorable Ruth Teichman, Chair.

Madam Chair, ladies and gentleman of the committee, it is a pleasure to be before you today not only as a proponent of this bill but for the first time as one of your colleagues. Senate Bill 333 is a piece of legislation that is very important to the residents of Sedgwick County and the state of Kansas. It is a simple piece of legislation with two sections. It requires the installation in automatic teller machines of a system which would allow the customer to initiate a distress signal being relayed to local law enforcement agencies in their jurisdiction. It is important to the residents of Sedgwick County and the state of Kansas due to the extraordinary nature of crimes perpetrated involving automatic teller machines and their customers. In an effort to deal with this issue in a comprehensive way, I've also introduced through the Committee on Judiciary, Senate Bill 438 which increases substantially the criminal penalties imposed for the crimes of robbery and aggravated robbery at an automatic teller machine. While many of us are aware of the violent and sadistic nature of the Carr murders in Wichita, other ATM crimes in Wichita have been similarly brutal. ATM crimes are not your normal everyday robbery where the criminal approaches the victim, demands money or property and then leaves upon receipt. These crimes tend to go on for hours, or even days, as the criminal must repeatedly approach the ATM machines to remove more and more money each time. In many cases, the victim is terrorized for an extended period of time far greater than a normal robbery.

My experience in the criminal justice system consists of working on over 60,000 criminal and traffic cases with over 20 years of experience in Kansas court. I practice mainly in the area of criminal and traffic law and have reviewed thousands of police reports. I have spoken with hundreds of victims of violent crime and understand in many respects the pain they are forced to endure. While I have some technical expertise, I certainly cannot address those issues to the level of our next witness, the inventor of this software program, Mr. Zingher is far more able to answer those technical questions in regards to his software.

I want to thank the committee for it's time and attention in this matter and I will stand for questions.

Respectfully submitted,

Phillip B Journey

Senate F I & I Committee
Meeting Date: FEB 5, 2004
Attachment No.: 8

Testimony of Joseph P. Zingher

Topeka, Kansas

February 5th 2004

I will begin by acknowledging that I have a financial interest at stake in the ATM crime issue because of my ownership of the SafetyPIN system. It is also true that the ATM industry has a financial interest at stake because the ATM industry, as of 2003, is a $14 Billion per year industry.

To begin with, an ATM network is simply a chain of computers passing messages back and forth with an ATM at one end and a computer with the account information at the other. All that an emergency PIN system would require is a new set of instructions being added to software already in place. There is no hardware change of any kind to the ATM or the computer. The SafetyPIN system could be installed nationwide in six months to a year at an estimated cost of $25 per ATM, (except in Kansas where it is now free). The average cost of a new ATM is $3500. Customers would be introduced to the system directly by their banks in their monthly statements. Finally, the system could and should be incorporated into the bank's advertising to fully educate the card holder and warn off criminals. The average ATM transaction takes 1.5 minutes. The average police response time to a legitimate 911 call is 2.5 minutes. That leaves one minute on average for the criminal to put as much distance between himself and the victim as possible.

The system itself will be as reliable, from the hardware or software standpoint, as the ATM network already is. The potential drawbacks of the system are 1) False Alarms; 2) Panicky Customers; and 3) Forgetful Customers.

The problem of False Alarms is well known to the police. There is no question that they are a problem in other circumstances. But, without having any hard statistical evidence to point to that shows the reverse PIN system will have a problem with it, the objection is mere conjecture. The burden of a false alarm cannot be weighed against the social benefit in deterring these crimes until it is actually deployed and used by the public. We do know there is a social cost in human lives and we know what will happen if nothing is done. The murders will continue. The SafetyPIN offers one advantage in this regard. You must strike each key in exactly the wrong order, otherwise, just as it does now, the computer interprets the entry as an error and the user is instructed to try again. Consider your own experience using a telephone keypad. Everyone has mis-dialed a number, but I've never turned the entire sequence around backwards and I doubt anyone else has. This is also true of PINs that are palindromes, such as 2442 and 7777. If your PIN follows the A-B-B-A pattern, then your emergency PIN is B-A-A-B so 2442 would result

in the Inside Out PIN 4224. Where all four digits are the same, 0000 through 9999, you would add 1 to each digit, so, 7777 would result in the Plus-1 PIN, 8888. Note that for these, you have to hit all four digits exactly wrong also. There is also an ergonomic factor at work when you type in your PIN. It just feels right.

The Panicky Customer objection needs to be examined closely. The Panicky Customer objection is a sophistry. It distracts from the real issue. It amounts to the claim that if the system is not perfect, then no one should have it. There are hundreds of thousands of ATM users in Kansas. A more rational analysis is that there will be three groups of people. The first group will never be able to use the system. The second group will be able to use the system sometimes and the third group will always be able to use the system. Those second and third groups generate a deterrence factor, because the criminal does not know in advance who can and cannot use the system. The first group therefore receives a benefit even if they can't use it personally. This deterrence affects not only the decision to commit the crime in the first place, but also the decision to murder the victim or hold the victim hostage while the account is cleaned out. The reason is obvious. The criminal doesn't know until it is too late that the alarm was given. As things stand now, the average ATM transaction takes 1 minute and 30 seconds. The average response time to a legitimate 911 call is 2 minutes and 30 seconds. That leaves one minute for the criminal to make his escape. Does he take the risk that the alarm was given, no matter what the victim says or does he take the money and run? As things stand now, there is virtually no chance of being caught. Even ignoring the deterrence effect, the increased likelihood of arrest will generate more arrests. If you catch the criminal, after the 5th crime and put him in prison, he does not continue committing crimes 6, 7, 8, etc. This is an overall net gain to society. With that in mind, I note that the Carr brothers were from Dodge. I doubt that the incident in Wichita was their first experience with ATM crimes.

The Forgetful Customer is an argument used in objecting to other types of emergency PIN systems. The ATM industry could adopt a system that has the card holder choose his own emergency PIN as well as his regular PIN. It might be years before the emergency PIN was needed, and in that time, the customer might simply forget what his emergency PIN is. This is a valid point in objecting to a generic emergency PIN, but, it would still have some deterrence. My system minimizes that problem by giving the victim a method of remembering the emergency PIN when needed, in effect, a mnemonic of sorts or memory aid. ReversePIN, Inside-OutPIN and Plus-1PIN are all intuitive and further, the card holder only needs to memorize one of the three. (If you've got too many PINs now, it's up to you to simplify your life.) With a reminder sticker on each ATM to prompt the card holder, the likelihood of being able to use the system when needed is radically improved. (This touches on an area known to police as "falling back on training".)

There's a legitimate question as to cost. It's free within Kansas. The software for the system, which I've brought with me today, is only three pages long. The reprogramming necessary to put it in place can be done in-house. There is no need to hire outside experts to do the programming. In point of fact, an emergency PIN system is already in use by

the ATM industry. The employee who loads the ATM is protected by an emergency PIN system already. Once integrated into the system, everything else is already in place. The police are notified through the burglar alarm company that already monitors the ATM. All that is needed is to route a message from the computer to the alarm company which calls the police department with all the relevant information. Some police departments are already making the conversion to cyber 911 calls. As that occurs, an even faster response time will develop. Please note that, as things stand now, there is no response at all. The reason that it is so cheap is that all the programming needed to make the system work is off-the-shelf technology.

It is also important to note that the system can be used when only an ATM card issued by a Kansas bank is used without interrupting the function of out-of-state ATM cards. That is, someone from Colorado driving through would be totally unaffected by the change over. You could literally have individuals in Kansas choosing to have the system or not. It could also provide some protection out-of-state as well without the out-of-state ATM company even being aware of the service.

I've found that the smaller banks and credit unions are the most receptive to this idea, even though in smaller towns, the danger is much less. The problems arose when they asked their own data processors to look into it. When they did, they were forced to withdraw from their contracts with us. They lacked the economic power to force their service providers to change the way they do business. For example, US Bank, which provides ATM data services for smaller banks, was asked to install the system by Heritage Bank in South Carolina. US Bank simply refused to even discuss it with them or with us. Glynn Teacher's Federal Credit Union in Georgia was also one of our early partners. They requested EDS to install the system. EDS wouldn't even discuss the matter with them unless they were paid $100,000 in advance. In essence, what I am saying is that the smaller banks are being held hostage to the dictates of the giant banks and ATM data processors.

The best that I can do is offer my explanation of what really motivates the ATM industry and explain why objections to the system are not legitimate.

Resistance to the adoption of an emergency PIN system for ATM users is rooted in the history of the ATM and in the legal liabilities that surround it. When ATMs were first introduced, they were so rare compared to today that it was impossible to say that they were a social problem at all. Following standard legal practice of large corporations, whenever a bank was sued over a crime at their ATM, they always settled the case and got a nondisclosure agreement before an appellate record could be created. (Note I said "bank" because the data processor is out of sight and out of mind.) This is the system that the bankers of today inherited and the way they have always done things. The bankers in charge today are not the ones who created the ATM industry. They inherited from the bankers who created it in the 1970's and early 80's. To even admit that a problem exists at all is counter to the established marketing doctrine. In fact, the American Bankers' Association has ceased giving out any numbers concerning the extent

of the problem, though they claimed in 1990, there were only 3000 ATM Crimes nationwide. The following year, the Los Angeles County Sheriff's Office estimated 2190 and the NYPD reported 743, leaving 67 for the rest of the country.

Most outrageous in all this is that people who don't even have ATM cards in the first place are also endangered. If you have an ATM card, you're aware that there is a danger. But, if you choose not to have an ATM card at all, that doesn't mean you're not going to be a victim of a criminal whose intent is to commit a forced ATM withdrawal. Few criminals ask their victim "Pardon me, but do you have an ATM card?" That means that everyone, ATM user or not, is placed at risk. 80% of these crimes begin as car-jackings from parking lots. The criminal doesn't learn until after taking the victim hostage that she or he doesn't even have an ATM card to begin with. The criminal still has a motive to commit murder though just to eliminate the witness. In essence, we all have to be paranoid about the problem because key executives in New York, Chicago, Los Angeles and San Francisco don't want to change their marketing doctrine.

I note that a similar situation faced the automobile industry in the early 1960's and again in the 1980's. Car manufacturers did not want to install seatbelts and safety-glass in cars because they didn't want to remind people that cars are dangerous, and that would hurt sales. It took Federal law to force a change on the industry. No one today would drive in a car without seatbelts and safety-glass. Later on, when air bags were invented in the late 1960's, the auto industry resisted installing them until after the patent had expired and they could get them for free. Still later, the inventor of anti-lock brakes couldn't market them to the auto industry, so they just allowed the patent to lapse. At which point, the auto industry instantly recognized how wonderful they were. I suspect that if Citibank owned my patent, they would offer it exclusively to their customers and charge extra for the service.

If you view the situation as a street crime, then logically, you cannot say that the ATM industry is accountable. If you view the situation as a business premise issue, then you logically come to the conclusion that the ATM industry is accountable. The ATM industry controls location, hours of operation and method of operation. It is their current method of operation that causes the problem. In the Wichita Eagle of April 19, 2001, a police captain from the Wichita PD and a criminologist from Ft Hays State University said that there is a deterrent value to this system. I suggest that it is now up to the ATM industry to prove why they are wrong.

There have been several political efforts over the years to make ATMs safer. In 1987, US Representative Mario Biaggi, a retired police lieutenant, proposed HR785, which would have directed the FBI to track ATM crimes and evaluate the usefulness of emergency PINs. The bill was simultaneously referred to Banking, Judiciary and Urban Affairs and died without even being debated in any of those committees. The next year, Mr. Biaggi was challenged in the primary and he lost. In 1994, the Chicago City Council passed an ordinance requiring banks to report ATM crimes to the police. In 1996, the Illinois Office of Banks and Real Estate declared it was illegal for the city to keep track of ATM Crimes. In New York and California, initiatives to force the adoption of panic

buttons on ATMs failed. Illinois, Texas and Nevada have adopted tort immunity statutes for ATM operators, ensuring that there will be no effort to improve safety. Those states have given permission to the ATM industry to kill people with impunity.

Whatever decision you reach here today will financially benefit one side or the other on this issue. I submit that only one decision has a benefit for the average citizen though.

The Kansas Bankers Association

2-5-04

TO: Senate Financial Institutions and Insurance Committee
FROM: Chuck Stones, SVP

Madam Chair and Members of the Committee,

The KBA appreciates the opportunity to appear before you today, in opposition to SB 333.

The banking industry has always been, and always will be, very concerned with the security of our customers. We just want to make sure that the measures we take will be effective. Such is the concern with the so called "SafetyPIN" system developed and marketed by Joe Zingher of Zi-Cube.

This product has been marketed by Mr. Zingher for several years, and to our knowledge, does NOT have a single bank customer. In recent years, Mr. Zingher has even offered his product for free. It appears that only one state has addressed this particular product legislatively. The State of Illinois passed a bill last year making implementation of the product optional or permissive.

The Banking Dept in Illinois did a legislatively mandated study of the "reverse PIN" system and found that - "a consumer may be under too much emotional stress to properly utilize the system, the system would be tremendously costly to implement both as to hardware and software requirements, quick response by police is not guaranteed, and no evidence exists that the reverse PIN system would actually reduce crime."

- Research shows that of all steps that can be taken to improve customer security, carful attention to the "3 L's", location, lighting and landscaping, plus education, produce the best results.
- This product has not been sold to any financial institution.
- Deterrent effect is over touted.
  Our customer may actually be in greater during the commission of a crime with the product in place.
- Remembering your PIN backwards, especially in a stressful situation, will be very difficult. This would place our customer in greater danger.
- This product is not as simple as is portrayed. Computer systems and national ATM networks will make this system very complex.

"In conclusion, significant barriers exist in the application of the reverse PIN system at this time. In addition, there appears to be no conclusive data or other information that shows that the reverse PIN system would serve to decrease ATM crime any more effectively than other security measures, if at all."

I assure you, our customers safety is the utmost importance to us. The banking industry has been diligent in implementing law enforcement recommendations regarding ATM safety, such as changes in location, lighting and landscaping. We have also been responsive by installing cameras at many ATM locations. We are concerned that the measures we take be effective. This particular product does not appear to meet that standard.

Thank you for your attention and we urge you to oppose this well intentioned, but misguided proposal

610 SW Corporate View, Box 4407 ♦Topeka, KS ♦ 66604-0407 ♦785-23
e-mail – cstones@ksbankers.com

Senate F I & I Committee
Meeting Date: FEB. 5 2004
Attachment No.: 4

Office of Banks and Real Estate

www.obr

Rod R. Blagoje

Agency Links

OBRE Home
Search OBRE
About OBRE
News
Lookup
Financial Literacy
Consumer Information
OBRE Bureaus
- Banks and Trusts
- Real Estate-Professions
- Residential-Finance

Legal
Discipline
Forms
Customer Service
OBRE Links

State Links

Search Illinois

Go

[Search Tips]

Inspector General

Agencies Boards and Commissions

Office of Banks and Real Estate

Section I.

Executive Summary

On May 26, 1999, Senate Resolution No. 134, offered by Senator Doris C. Karpiel, was adopted by the Senate. The resolution requests the Office of Banks and Real Estate to study safety and security issues surrounding the use of automated teller machines ("ATMs") by consumers. In particular, Resolution No. 134 requests the Office of Banks and Real Estate to report on the relative merits of a particular ATM security devise, the reverse PIN safety system. Accordingly, this report does not address other related technology such as shared networks, point-of-sale terminals, or "smart" cards.

ATM use continues to grow at a staggering rate. These machines extend traditional banking hours by dispensing cash and making other transactions available 24 hours a day. Approximately 12 billion ATM transactions take place per year at thousands of ATMs.

Although there is no precise data on ATM crime, violent crime against ATM users is relatively rare. Over the decade of the 1990s, ATM crime has actually decreased from approximately one crime per one million ATM transactions to one crime per 3.5 million transactions. At the same time, the use of ATMs has significantly increased. Nevertheless, public perception of significant crime at ATMs exists. To deal with the crime that does occur, the General Assembly adopted the Automated Teller Machine Security Act in 1996 which deals with the main concerns of ATM safety and security – location, lighting, and landscaping. This legislation provides a safe harbor from legal liability to ATM operators with regard to security matters.

Technological advances have brought about proposals for additional ATM security measures. These include enclosed ATM structures, closed circuit television cameras, biometrics, alarm or "panic" buttons, and telephones at ATMs. The reverse PIN warning system is one of these security measures.

An analysis of the reverse PIN warning system is specifically requested by Resolution No. 134. The reverse PIN system attempts to utilize current technology to provide law enforcement with the immediate location and background information concerning a potential victim. However, a consumer may be under too much emotional stress to properly utilize the system, the system would be tremendously costly to implement both as to hardware and software requirements, quick response by police is not guaranteed, and no evidence exists that the reverse PIN system would actually reduce crime.

Recommendations

Agency Overview

Key Contacts
Annual Report (PDF File)
Agency News
Discipline
License Info
Employment Info
Related Sites
U.S. Census Demographic Info

The Office of Banks and Real Estate recommends:

1. That the relevant law enforcement agencies gather statistical and other data concerning ATM crime. At present, it is difficult, if not impossible, to recommend additional safety measures for ATMs because of a lack of reliable data. Reports of ATM crime are usually included as part of larger categories such as theft or robbery.
2. That the financial services industry, the law enforcement community, consumer protection groups, and other interested parties study whether the reverse PIN system is suitable and desirable for use in this field.
3. That statutory proposals affecting ATM security be introduced as amendments to the ATM Security Act to maintain the comprehensive nature of the Act as to ATM security matters.

Section II.

Automated Teller Machine Security

A Brief History of Bank Security

Historically, banks have been targets for economic crimes. As the U.S. economy developed from a barter to a currency based system, financial institutions assumed a risk of loss proportionate to the increase in use of paper money. Exchange and storage of currency created a new area of concern for banks: security for these assets. Banks initiated security systems and continually adapted them to meet changing needs.

Bank security has largely been a matter of privately funded protective services [as opposed to public law enforcement] to safeguard life, property, and business interests against crime. Private security includes protective services and devices, and private resources necessary to investigate crime. The nation's first banks relied on an unsophisticated watchman service for nighttime protection or required the cashier to live on the bank premises for safety of the bank's assets. Today, the banking industry has available for its use a well-rounded contractual security system offering alarm, armored car, guard, and investigative protective services.

Expanded Use of Debit Cards

Since the introduction of the first automated teller machine ("ATM") debit cards in the early 1970s, significant electronic technological progress has occurred in the banking and financial industry. Consumer acceptance of electronic banking continues to drive many developments in the financial industry. The financial community continues to offer new electronic banking and money services to a population of households who are

becoming more literate in electronic banking concepts. Government regulation also contributes to an increasing number of debit card users. For example, beginning in 1996 all federal government payments to people newly receiving salary or benefits and all payments to companies for new contracts with the federal government must be made electronically. Typically, many people not having a debit card who start receiving funds from the government electronically will become new debit card users. In addition to protecting currency and guarding against electronic fraud, there must be a continuous risk assessment of personal safety factors to ATM service employees and consumers who use ATMs by banks and ATM operators.

Automated Teller Machines

ATMs extend traditional banking hours by dispensing cash and making other transactions available 24 hours a day. At the beginning of 1974, there were only 1,656 operating ATMs nationwide. Today, online debit cardholders initiate approximately 12 billion ATM transactions per year at thousands of ATMs.

As electronic debit card transaction volumes continue to increase with the installation of more ATMs, banks must adopt special security considerations for the ATM environment. On-premises ATMs (those typically located in bank lobbies) provide the most suitable working environment for the consumer. The trend towards installation of free standing machines in shopping malls, in free standing kiosks in parking lots, supermarkets, and office buildings obviously presents a whole new array of security problems for ATM operators.

Security Considerations for Debit Card Installations

Currently, major law enforcement agencies do not regularly keep track of ATM crime. Most assaults related to ATM usage are included in larger general categories for assault, battery and the like. Special studies conducted from time to time have shown a relatively low rate of ATM crime. Although there is no precise data as to the extent of violent crime perpetrated against the users of ATMs and night depositories, assaults on bank customers who use these facilities occurs infrequently. It is estimated that currently about one in every 3.5 million ATM transactions result in a robbery of the customer. This is less than the estimated one in every million transactions occurring in 1989. While crime at or near ATMs may not be on the rise, public fear of ATM-related theft is increasing.

ATM crime is a street crime conducted at an ATM. Most ATM robberies occur at night between 8:00 p.m. and midnight. Most robbery victims are women, are alone when robbed. Most claim they never saw the robber coming. The typical ATM robber is 25 years of age, works alone, and usually positions himself nearby waiting for a victim to approach and withdraw cash.

Extensive research by the American Bankers Association has

shown that of all steps that can be taken to improve customer security, careful attention to the "three Ls," location, lighting, and landscaping, produce the best results.

* **Location Guidelines**

The location of ATMs is the single most important issue relative to customer safety. In determining the placement of new ATMs, the following guidelines are recommended:

- Design the site so that customers using the machine have high visibility of their surroundings.
- Design vestibules so as not to limit visibility of customers while using the ATM, evaluate the following: use of convex mirrors and minimal use of solid walls and blinds.
- Place ATMs near well-lighted parking areas.
- Place ATMs where they will have "drive-by" visibility from all nearby parking lots, walkways, and main thoroughfares.
- Prepare a crime profile of the area around the ATM.

* **Lighting Guidelines**

The following are suggestions for lighting levels needed to achieve effective customer safety. Lighting intensity is measured in footcandles ("F.C."), or candlefeet.

- Within a 5-foot radius of the ATM, maintain a 10 F.C. minimum, measured at 36 inches above ground.
- Within 50 feet of the ATM, including the nearest available parking location, maintain a 2 F.C. minimum, measured at 36 inches above ground.

* **Landscaping Guidelines**

- Plant slow-growing shrubbery that needs trimming less frequently.
- Trim shrubbery to a maximum of 24 inches above ground level. Trees should be "branch free" below the 6 foot level.
- Monitor the growth of shrubbery on a regular schedule.
- Assess the placement of other objects that could block vision (e.g., walls, benches, and dumpsters).

* In addition to the "three Ls," education is one of the best ways to deter ATM crime. Surveillance cameras and other devices can lead to a false sense of security among consumers. Customers will avoid crime if they only use ATMs at certain times and locations. Not using ATMs in poorly lit locations at night alone will deter crime.

Section III.

Reverse PIN Warning Safety System

Most customers obtain ATM service by inserting a card into a machine and entering a personal identification number, commonly referred to as a "PIN." The reverse PIN warning safety system is one product that claims to offer added security to customers in the event of a robbery while using their ATM. Zi Cubed, Inc. (www.zicubedatm.com) markets the SafetyPIN ATM security system, a reverse PIN safety system. On March 24, 1998, a patent was issued for this product.

How the Reverse PIN System Works

ATM card issuers typically issue one PIN to a customer. Under the Zi Cubed system, customers are assigned an emergency second PIN which is usually the reverse of their original number. For example, if 1234 were an individual's PIN, then the emergency PIN would be 4321. If the PIN were 2442, then the emergency could be 4224. If the emergency PIN is entered, presumably during a robbery, the ATM processing main computer sends a distress message to the local police department. In addition to the location of the ATM, police could find out who the customer was with information taken from the customer's bank account records. Police could also access a description of the customer from the Secretary of State's Drivers' Services Division. By the time police reach the ATM they would know who the customer is, what s/he looks like, and where s/he lives.

The reverse PIN system has not been sold to any financial institution yet. Marketing efforts have centered around customers' fear of ATM crime and on ATM operators' fear of litigation for failure to take sufficient safety precautions.

Analysis

A 1993 special study by the Chicago Police Department shows that 47 ATM crimes were committed that year in Chicago, the jurisdiction with the largest number and concentration of ATMs in the Illinois. The trend of ATM crime has declined. However, public perception appears to be that ATM crime occurs more frequently. Adoption of the Zi Cube system may alleviate some customers' fear of crime, whether real or perceived.

** The deterrent affect of having such a system in place is another touted feature of the system. However, deterrence does not prevent crime in progress. More importantly, the law enforcement community does not generally encourage resistance or confrontation to thwart theft or robbery. The risk of physical harm to the customer is greatly increased should they resist. When coupled with the fact that ATMs generally limit withdrawals to

approximately $200.00, engaging a criminal in an altercation or otherwise offering resistance over such an amount does not appear to be prudent.

Protection from lawsuits is another claim of the Zi Cube system. The distributor claims that merely installing this system will help rebut lawsuits alleging that ATM operators are negligent in providing safety to customers. While this argument may possess some merit in other states, this argument is not as compelling in Illinois. Traditional legal defenses and safe harbor provisions contained in the Illinois ATM Security Act available to ATM operators will likely reduce litigation in this area. See, Section V - ATMs and the Law.

Finally, human behavior must be taken into account. Being surprised by the threat of bodily harm is extremely stressful. Severe stress such as this impairs the thought process. Under these conditions, it is difficult enough for many people to remember their correct PIN number. It may be asking too much of a consumer to try to remember a second emergency PIN. Criminals will undoubtedly be among the first to know of a reverse PIN system and how it works. Any delays or glitches incurred by a victim during an ATM crime could cause the criminal to physically harm the victim.

Computer Interface Barriers

Computer interface problems are estimated to be significant and costly in implementing the reverse PIN system at this time. First, are the limitations inherent in the use of PIN numbers. The system would double the amount of PINs used per person.

Second, conversion to this system requires a significant commitment in resources to writing new computer software programs that recognize the reverse PIN and then make multiple complex decisions. Currently, ATMs communicate with banks and make what are termed "binary" (i.e., simple "yes/no") decisions concerning the account and transaction information. Under the reverse PIN system, the main computer must: (a) determine and communicate with the police station closest to the ATM; (b) the computer must communicate with the bank account of the cardholder and obtain account information that is usually confidential and protected (this process is more complicated if the ATM is not from the accountholder's bank); and, (c) the main computer must then also communicate with the Secretary of State's office for driver license information.

Third, most law enforcement agencies do not have the computer capacity to provide the necessary real time communication with an ATM. Many police 911 units respond only to voice communication, although some are now taking calls via the internet. In addition, there is no assurance of immediate response by police agencies. This may result from the huge number of calls handled in urban areas to the geographic separation that occurs in rural locations.

Fourth, the cost to reconfigure the ATM system, including shared ATM networks, can be quite high. There are over 5,000 ATMs

under regulation by the Office of Banks and Real Estate. The physical reconfigurations needed to make changes to machines have been estimated at $1,500.00 to the thousands of dollars each. The minimum impact is estimated to be at least $7,500,000.00. This does not include the software programming costs. This estimate does not include the additional costs associated with thousands of ATMs in Illinois that are not regulated by the Office of Banks and Real Estate. Too be fully functional, the Zi Cube system would have to have communication capabilities with financial institutions worldwide in order obtain customer account information. The system would likewise have to communicate with driver license agencies or similar authorities worldwide to obtain descriptive information about the victim.

In conclusion, significant barriers exist in the application of the reverse PIN system at this time. In addition, there appears to be no conclusive data or other information that shows that the reverse PIN system would serve to decrease ATM crime any more effectively than other security measures, if at all. Nevertheless, should individual ATM operators and networks conclude that the reverse PIN system provides benefits that justify the significant costs associated with it, they may adopt such a system. Such reasons may include market competition, consumer demand, experiences with lawsuits, or improved technology.

Section IV.

Prior Studies

ATM use continues to grow at a staggering rate. At the same time, crime rates have dropped from an estimated one in one million transactions in the early 1990s to one in 3.5 million transactions in 1999. The late 1980s and early 1990s saw a growth in the amount and perception of ATM crime. As a result, in 1990 and 1993, the City Council of Chicago conducted extensive studies as ordinances dealing with ATM security were considered. The ordinance adopted was superseded by the Illinois ATM Security Act. See, Section V – ATMs and the Law. Many of the findings and recommendations of these studies, however, are still considered relevant today by persons involved in the field of ATM security. Accordingly, a summary of these studies is included here.

1990 City of Chicago ATM Security Advisory Committee Report

The ATM Security Advisory Committee highlighted six conclusions:

1. No widespread incidence of robbery or assault at ATMs exist.

2. Financial institutions have responsibly provided for consumer safety in terms of guards, restricted access

and/or combinations of these.

3. Current ATM users are generally satisfied with current safety provisions at ATMs.
4. There is room for improvement in communications between the Chicago Police Department and financial institutions with respect to identifying ATM crime trends and preventing ATM crime.
5. No additional technological enhancements are available and practical to enhance ATM security (911 applications were explored, but were deemed inappropriate because they were only available for voice communications and no proof existed that they could prevent crime).
6. It would be inappropriate to mandate uniform ATM standards since all sites are different.

The Committee made four recommendations:

1. The Chicago Police Department and financial institutions should establish formal procedures to:

   a. track ATM trends
   b. enhance communications
   c. cooperatively determine incremental crime prevention strategies, including:
   d. The Chicago Police Department should appoint a liaison for ATM issues (initially the Deputy Chief of the Administrative Section of the Detective Division).
   e. The Chicago Police Department should collect, analyze, summarize, and make available all data on incidents of ATM crime to determine trends and assist in future prevention of ATM crime and apprehension of perpetrators of ATM crimes.
   f. The Chicago Police Department should receive and review through the wall 24 hour access ATM building permits obtained from the Dept. of Buildings and, when appropriate, advise the deploying financial institution of security concerns.
   g. The Chicago Police Department should develop training programs on ATM security for police personnel and community groups.

2. All Chicago financial institutions should be given an ATM security checklist that encompasses issues that need to be considered regarding safety (e.g., lighting, cameras, crime frequency in area, hours of availability, etc.).
3. The Chicago Police Department and financial institutions should meet semi-annually to review ATM security, stay abreast of emerging security technology and evaluate their practical applications for ATMs.
4. Consumer education brochures should be circulated to all Chicago area financial institutions.

1993 City of Chicago ATM Security Advisory Committee Report

The ATM Security Advisory Committee highlighted seven conclusions:

1. ATM crime had not increased in recent years.
2. Most financial institutions had provided responsibly for consumer safety at ATMs through use of guards, cameras, and/or restricted access devices.
3. Consumers were generally satisfied with current ATM safety provisions and did not perceive that ATM safety had deteriorated over the three previous years. They feel that they are responsible for taking steps to ensure their own personal safety at ATMs and would object to the mandatory closure of all ATMs at night.
4. Communication between the law enforcement community and financial institutions seems to be effective although there is not now a formal vehicle for this communications.
5. There were no technological enhancements that, if mandated, would materially help to prevent ATM crimes from occurring or help law enforcement officials intervene during crimes in progress. In fact, many technological enhancements aimed at intervention (e.g. panic buttons) would likely just result in the movement of crime to different locations where victims are more susceptible.
6. Mandating the deployment of ATMs in all police and fire stations would not be appropriate for various logistical reasons.
7. It would be inappropriate to mandate uniform safety standards for all ATMs since there is a wide diversity in types and locations of ATMs. Nevertheless, certain minimum standards would be appropriate for ATMs that are either exposed to the street or located in an unmanned structure, the sole purpose of which is to enclose the ATM.

The Committee recommended that the City Council consider adoption of an ordinance that would mandate certain minimum safety provisions for financial institutions.

1. Adopt procedures for evaluating safety at ATMs which are exposed to the street or located in a building, the sole purpose of which is to enclose the ATM. The procedures should consider:

    - lighting
    - visual obstructions in the areas around the ATMs
    - incidence of crime in the vicinity of the ATM as reflected in the records of local law enforcement agencies and the institution's own internal records

1. Comply with minimum lighting standards at all outdoor ATMs and all ATMs located in structures, the sole purpose of which is to house the ATM.
2. Distribute ATM safety precaution information to each of their cardholders.
3. Furnish, upon request by the City Council, information regarding an institution's compliance with the provisions of the ATM security ordinance and information on ATM crime incidents at specific ATM deployed by the financial institution.

Wednesday, February 4, 2004

ATM Safety Tips

from the ABA Education Foundation

The automated teller machine (ATM) revolution has made banking more convenient today than ever before. With the touch of a few buttons, you can withdraw cash, make deposits and transfer funds virtually anywhere an ATM is located.

The Bank's Role

To ensure customer safety at ATMs, banks are putting ATMs in areas that are visible by passers-by, trimming landscape to prevent potential criminals from hiding, and installing or upgrading lighting that is bright enough for use at night.

Some banks also have installed cameras, rear-view mirrors, panic buttons and special signs. And most banks limit the amount of cash that can be withdrawn on a daily basis.

The Customer's Role

Bank customers should always use common sense when using an ATM. These tips are a start, but the best advice is simply not to use an ATM if you feel at all uncomfortable doing so. ATMs provide convenience, buy they haven't replaced the bank teller. If you prefer, conduct your business in the bank lobby.

Exercise care when using an ATM, and follow these general rules:

Protecting Your ATM Card

- Always protect your ATM card and keep it in a safe place, just like you would cash, credit cards or checks.

- Do not leave your ATM card lying around the house or on your desk at work. No one should have access to the card but you. Immediately notify your bank if it is lost or stolen.

- Keep your Personal Identification Number (PIN) a secret. Never write it down anywhere, especially on your ATM card.

- Never give any information about your ATM card or PIN over the telephone. For example, if you receive a

call, supposedly from your bank or possibly the police, wanting to verify your PIN, do not give that information. Notify the police immediately.

Using an ATM

- Be aware of your surroundings, particularly at night. If you observe or sense suspicious persons or circumstances, do not use the machine at that time.

- Have your ATM card ready and in your hand as you approach the ATM. Don't wait to get to the ATM and then take your card out of your wallet or purse.

- Be careful that no one can see you enter your PIN at the ATM. Use your body to "shield" the ATM keyboard as you enter your PIN into the ATM.

- To keep your account information confidential, always take your receipts or transaction records with you.

- Do not count or visually display any money you received from the ATM. Immediately put your money into your pocket or purse and count it later.

- If you are using a drive-up ATM, be sure passenger windows are rolled up and all doors are locked. If you leave your car and walk to the ATM, lock your car.

Special Precautions for Using an ATM at Night

- Park close to the ATM in a well-lighted area.

- Take another person with you, if at all possible.

- If the lights at the ATM are not working, don't use it.

- If shrubbery has overgrown or a tree blocks the view, select another ATM and notify your bank.

ATM Crime

These tips are meant to make you aware that although rare, ATM crime can happen. Preventing such a crime must be a cooperative effort between you and your bank.

ATM SAFETY TIPS

Safety Tips for Using an ATM

The automated teller machine (ATM) provides quick, convenient access to your money. By following these important safety tips, you can safely use the ATM whenever you need cash.

- **Memorize your Personal Identification Number (PIN).** Do not write your PIN on your ATM/debit card or leave it in your wallet.
- **Keep your PIN a secret.** Someone you trust today may not be trustworthy tomorrow. If you suspect unauthorized use of your card, notify your financial institution immediately.
- **Stand between the ATM and people waiting to use the machine,** and shield the keyboard so others can't see you enter your PIN.
- **Always take your ATM receipt with you** or shred the receipt before discarding it. Receipts may contain valuable account information that should be safeguarded.
- **When using an ATM after sunset, consider going with another person to an ATM in a well-lighted area.** If someone in the area looks suspicious, cancel your transaction, retrieve your ATM/debit card and immediately leave the area. Choose another ATM in a safer area.
- **Have your transactions ready before going to the ATM.** Fill out your deposit slip, place your checks or cash in an envelope and seal it before you arrive at the ATM location.
- **Have your ATM/debit card ready to insert into the machine before arriving at the ATM** so you don't have to reach into your purse or wallet while standing in front of the ATM.
- **Don't fall for "con" games**. If anyone asks you to withdraw money for any reason, leave the area at once. Notify your financial institution and local law enforcement officials immediately of any criminal activity.
- **Never give information about your ATM account to strangers** or inquirers on the telephone. Communicate this information only to your financial institution in person.

PULSE Urges ATM Cardholders to Follow Common Sense Safety Tips When Getting Cash

Incidence of crime is relatively rare, and often preventable

Consumers today are enamored with the "anytime, anywhere" nature of automated teller machines (ATMs), and while the convenience of using these terminals has made them the preferred method of getting cash, their use is not to be taken lightly, according to a leading electronic funds transfer network. PULSE EFT Association, which processes more than 45 million ATM and point-of-sale (POS) transactions each month, is reminding cardholders to follow simple common sense ATM safety guidelines to assist in minimizing the risk of crime.

"In a shared network like PULSE, both card issuers and ATM operators share a responsibility to educate consumers on the 'safe' use of ATMs and to maintain ATM environments that are consistent with industry standards and applicable laws," said Stan Paur, president and CEO of PULSE. "It's a good idea for consumers to take time to review their habits to make sure they routinely take appropriate precautions when accessing their cash."

With the growing availability and popularity of ATMs, consumers across the country can benefit from the following common sense recommendations from PULSE:

Security At Walk-Up ATMs

- *Always observe your surroundings before conducting an ATM transaction. Observe the entire area from the safety of your car before getting out. If anyone or anything appears to be suspicious, leave the area at once.*
- *If an ATM is obstructed from view or poorly lit, go to another ATM. It's a good idea to take a companion along when using an ATM, especially at night.*
- *Minimize time spent at the ATM by having your card out and ready to use. Do not let anyone see how much money you withdrew and never count your money while at the ATM.*
- *Never allow a stranger to assist you in conducting an ATM transaction, even if you have trouble or if your card is stuck.*
- *Stand between the ATM and anyone waiting to use the terminal so that others cannot see your secret code or transaction amount.*
- *If you see anyone or anything suspicious while conducting a transaction, cancel your transaction and leave immediately.*
- *Look for possible fraudulent devices attached to the ATM. If the ATM looks different or appears to have any attachments over the card slot or PIN pad, do not use the ATM.*

Security At Drive-Up ATMs

- *Keep the doors locked, windows up and engine running at all times when waiting in line at a drive-up ATM.*
- *Leave enough room between cars to allow for a quick exit should it become necessary.*
- *Before lowering the window to use an ATM, observe the entire surrounding area. If anyone or anything appears to be suspicious, drive away at once.*
- *Minimize time spent at the ATM by having your card out and ready to use. Once your transaction is complete, take your money, card and receipt and immediately drive away from the terminal.*
- *While conducting a transaction, if anyone or anything appears suspicious, cancel your transaction and leave immediately.*
- *If anyone follows you after making your ATM transaction, go immediately to a crowded, well-lit area and call the police.*

Industry data indicates the relative incidence of ATM crime nationwide dropped from one-in-1 million transactions in 1990 to one-in-3.5 million transactions by the end of the decade. While these statistics show that it is unlikely any particular cardholder will ever be involved in a crime at an ATM, the financial services industry encourages all consumers to keep safety in mind when using ATMs.

PULSE is one of the nation's leading shared electronic funds transfer networks, serving more than 2,100 banks, credit unions and savings and loans across a nine-state primary service area including Alabama, Arkansas, Colorado, Louisiana, Mississippi, New Mexico, Oklahoma, Tennessee and Texas. The network links an estimated 45 million cardholders with more than 46,000 ATMs and 236,000 point-of-sale terminals in all 50 states.

Contacts: Mary Brown
Senior Vice President
PULSE EFT ASSOCIATION
(800) 420-2122

Ellen Read
Ben Flusche
READ-POLAND ASSOCIATES
(800) 472-4122

HEARTLAND COMMUNITY BANKERS ASSOCIATION

Matthew S. Goddard, Vice President

700 S. Kansas Ave., Suite 512
Topeka, Kansas 66603
Office (785) 232-8215 • Fax (785) 232-9320
mgoddard@hcbankers.com

To: Senate Financial Institutions and Insurance Committee

From: Matthew Goddard
Heartland Community Bankers Association

Date: February 5, 2004

Re: Senate Bill No. 333

The Heartland Community Bankers Association appreciates the opportunity to share its opposition to Senate Bill 333 with the Senate Committee on Financial Institutions and Insurance.

The bill mandates that any ATM operated in Kansas must be programmed to send an alarm to local law enforcement anytime a consumer enters his or her personal identification number (PIN) in reverse order. HCBA and our member institutions are committed to providing ATM users with a safe banking experience. We are opposed, however, to legislation requiring ATM owners to use a specific and unproven security program.

HCBA agrees that ATM safety is an important issue and our members strive to make ATM's as safe as possible. A common security consideration when placing ATM's is the three "L's" – location, lighting and landscape. Successfully addressing these issues can help deter possible criminal acts. Unfortunately, criminals sometimes still commit crimes against ATM users. We are unconvinced that SB 333 would be an effective response to this possibility.

It is the understanding of HCBA that the reverse-PIN software is a product offered by an Illinois company. It is further our understanding that this company received a patent for its product, SafetyPIN, in 1998 but since then no financial institution has agreed to use it. This leads us to believe that the product may not be the panacea it is marketed to be. This lack of significant real world usage certainly does not warrant legislation such as SB 333 that mandates its use.

In 1999 the Illinois State Senate requested a study of safety and security issues surrounding the use of ATM's. Part of the study focused on the reverse-PIN system. The study stated:

> *In conclusion, significant barriers exist in the application of the reverse PIN system at this time. In addition, there appears to be no conclusive data or other information that shows that the reverse PIN system would serve to decrease ATM crime any more effectively than other security measures, if at all. Nevertheless, should individual ATM operators and networks conclude that the reverse PIN system provides benefits that justify the significant costs associated with it, they may adopt such a system.*

The Illinois study questioned the overall effectiveness of SafetyPIN. For example, many

Senate F I & I Committee
Meeting Date: FEB 5 2004
Attachment No.: 5

customers have trouble recalling their PIN number in normal situations. Would a customer under duress, threatened with physical violence, have the presence of mind to enter their PIN backwards? If the stress of the situation resulted in the customer entering an incorrect reverse PIN and the transaction was denied, would that put the customer in greater physical danger? SafetyPIN still gives customers their money, so the criminal can escape with the money before police arrive on the scene.

The effectiveness of SafetyPIN would be greatly diminished as criminals become aware of it. Rather than acting as a deterrant, criminals could simply rob their victims **after** they use the ATM. Unfortunately, criminals can be very adept at keeping pace with increased security measures. A reverse-PIN system would not necessarily reduce crime.

HCBA has a number of practical concerns with SB 333 and the SafetyPIN program:

- Most ATM's are monitored by a security system, but alarms operate independently of the software that runs the ATM. In other words, the ATM's alarm cannot be triggered by typing on the keypad. In the event a reverse PIN is entered, the ATM processor would have to notify the alarm company who in turn would have to notify law enforcement. There is no direct connection between the ATM and local law enforcement.

- Many financial institutions allow customers to select their own PIN. Numbers like 7777 or 1331 may confuse customers when they are under duress.

- There is no way of knowing if a person is simply entering their PIN in the wrong order. Police will have to be dispatched simply because a customer transposes their PIN.

- The data processor running the ATM software does not necessarily have access to a bank customer's account information. The processor does not even know the customer' name. Law enforcement would have to contact a bank employee to learn any information about the victim.

- There are many non-bank ATM's. Some ATM's, often including those that don't belong to a financial institution, do not conduct transactions in "real time." This means the ATM would be unable to send a timely warning even if a reverse PIN is entered. Customers could have a false sense of security.

Again, security for ATM customers is a serious matter for HCBA and our members. The steps we take to protect our customers are designed to be effective. The reverse-PIN technology has not shown that it meets that standard. Legislation is not needed to allow ATM owners to try the technology for themselves. A government mandate is not needed and is, in fact, unwarranted.

The Heartland Community Bankers Association appreciates the consideration of our concerns by the Senate Financial Institutions and Insurance Committee.

TO: Senate Financial Institutions and Insurance Committee
FROM: K.C. Blodgett, Supervisor of Security Personnel, Commerce Bank and Trust, Topeka.

K. C. Blodgett, retired Topeka Police Lieutenant with 28 years of service.
During my career I was assigned to the Patrol Division, K-9 Officer, Drug Enforcement Unit, Detective Division assigned to Part 1 Crimes which include Homicide, Agg. Assault, Rape, and Agg. Robbery. Other areas: Hostage Negotiator and Instructor in the Topeka Police Department Academy primarily in the area of Narcotic Enforcement. Assoications: Past President of the National Drug Enforcement Officers Association, Past President and organizer of the Kansas Narcotic Officers Association, Past President of Topeka Lodge
#3 Fraternal Order of Police, and presently the State President for the Kansas Fraternal Order of Police representing over 2700 Law Enforcement Officers throughout Kansas.

For the past 17 years I have been employed by Commerce Bank & Trust as a Security Guard, for the past 8 years I have been the supervisor for Security Personnel. Also employed by the Kansas Highway Patrol assigned to Troop B as a Special Investigator.

SB 333 which deals with "reverse PIN" security systems on all ATM's.

I can only speak of my past experience within the Law Enforcement Community.
One primary rule which all Law Enforcement teaches the public is to "cooperate" in any given situation when dealing with the criminal element.
During my career with the Topeka Police Department I had the opportunity to speak to many citizen organizations and questions would alway come up on what to do if they had a home invasion, were robbed, if someone were to "car-jack" their car, or in general what to do when confronted by a criminal.
No matter what type of situation I was asked about the answer was always, "cooperate with them"!!!!!

I feel that there are several concerns I would have as a retired Law Enforcement Officer with SB 333. One would be the ability of an individual to reverse their PIN in a stressful situation. Another situation would be if the individual would be approached and the thief would indicate someone was watching the victims' residence, if a phone call was not made within a certain amount of time that the victims' family would be harmed. And lastly, if the police were to respond and catch the criminal in the act we could have a "hostage situation". All of these situations could result in an injury to the victim or their families. Again, we are taught in the Law Enforcement field to have the victims of crimes to cooperate.

In working with Financial Institutes for the past 17 years it is very clear that there are safeguards already in place such as the limit on the amount an individual can receive from an ATM and a time limit that a certain amount can be withdrawn. Another question would be regarding the number of incidents when citizens have had this happen to them. My experience would indicate that this is not a common crime. The most common incident is where the thief watches the victim receive the money and then approaches them and takes their money. These types of crimes are crimes of opportunity. I know of only one incident in which a person was at an ATM and robbed, this was after the removal of funds from the ATM.

My personal belief is that SB 333 would not be beneficial to anyone, the victim, the Financial Institutes, or Law Enforcement.

Senate Financial Institutions and Insurance Committee
Thursday, February 5, 2004

Hearing on SB 333 Regarding ATM Reverse PIN Technology

Comments of Commerce Bank of Kansas City and Intrust Bank
Submitted by Ron Gaches
Gaches, Braden, Barbee & Associates

Senator Teichman and members of the Committee, thank you for this opportunity to appear before you committee and express our concerns about the reasonableness of SB 333.

Maintaining the personal security of their customers is the highest concern of our bank clients. To the end, our clients have spent millions of dollars in the design and construction of the most modern and secure bank facilities possible, including ATM locations. Where specific ATM locations have been identified as posing a heightened risk of injury or theft, we have made investments in lighting, cameras, and improved access to provide improved security. In some occasions, ATM locations have been moved to address security concerns.

The reverse PIN technology mandated in SB 333 has not been demonstrated to improve the security of ATM users. It is worth noting, that mandates similar to this one have been discussed in several states but adopted by no one.

The practical obstacles to making such technology effective are several. For example, the ATM units operated by Commerce are dumb terminals. They are not capable of sending an alarm based on a message keyed into the machine by the customer. Some units do have internal alarms, but they are triggered by interaction with the hardware components. Many also have seismic and heat detection capabilities. The lock mechanisms are mechanical and are connected to alarms, but not electronically integrated to other systems.

At our customers' request, we permit real-time changes in the customer's PIN. The SB 333 mandate creates several technology challenges associated with keeping the customers PIN changes synched up real time with the reverse PIN. We have not seen technology that would permit the wide variety of our ATM machines to be adequately modified to fully comply with the requirement and retain the PIN flexibility requested by our customers.

Finally, we believe human error creates an opportunity for multiple false alarms or, even worse, inability of the customer to respond to threatening occasions with a clear mind. Unfortunately, technology is not the answer to every problem. We ask that you oppose this mandate.

KANSAS CREDIT UNION ASSOCIATION

Madam Chairman, members of the committee, I am Bill Henry, Director of Government and Regulatory Affairs for the Kansas Credit Union Association and I appear today with questions on SB 333.

Credit unions operate automated teller machines throughout the state of Kansas through cooperative networks that allow members to withdraw cash and make deposits at various sites.

Member safety is of the utmost importance to credit unions and the sponsors of SB 333 should be complimented for their purpose in introducing this legislation.

One state to date has adopted legislation similar to this measure—the state of Illinois in 2003 but that measure was permissive. Since the passage of that legislation no financial institution in that state has adopted the use of PIN software that would allow an individual by reversing his or her personal identification number to give an alarm that would alert law enforcement to a robbery. That is despite the fact that the holder of the patent to this software has said he would offer it free to financial institutions in that state.

The reasons for this may be varied but we believe for this idea to be functional it would need to be implemented industry-wide and nation-wide. The reason for this is due to the sheer number of various networks involved in ATM deployment. For example in Topeka alone where a group of credit unions have gone together to operate 60 machines there are six different networks involved in servicing those machines. Each of the networks has different operating protocols and there is also the question of whether each network has the capability of identifying the machine where the robbery may be going down.

We are still seeking more data from suppliers of ATM equipment but as an industry we need more time to consider the impact and ramifications of this legislation.

We have been told by one of the ATM networks that it will require "significant development both in time and expenses" to program their system and they do not have the capability today to provide that support.

We were also told by network experts that the expense of doing this program and implementing it on a state by state basis would be far greater for development than having all financial institutions across the United States share in the cost.

Until these questions can be answered the Kansas Credit Union Association believes SB 333 should not be recommended favorable for passage.

650 S. Westdale Drive
Suite 100
Wichita, Kansas
67209-2570
1-800-362-2076
Tel 316-942-7965
Fax 316-206-2203

Topeka Office
816 SW Topeka Blvd.
Topeka, Kansas
66612-1635
1-888-482-5282
Tel 785-232-2446
Fax 785-232-2730

Senate F I & I Committee

Meeting Date: FEB 5 2004

Attachment No.: 8