

**REPORT OF THE DIVISION OF MOTOR VEHICLES
AND DEPARTMENT OF STATE POLICE ON THE
FEASIBILITY OF REQUIRING A THUMBPRINT ON
DRIVERS' LICENSES AND IDENTIFICATION CARDS
TO
THE GOVERNOR
AND
GENERAL ASSEMBLY OF VIRGINIA**



**HOUSE DOCUMENT NO. 6
COMMONWEALTH OF VIRGINIA
RICHMOND
1982**



COMMONWEALTH of VIRGINIA
Division of Motor Vehicles
2300 West Broad Street

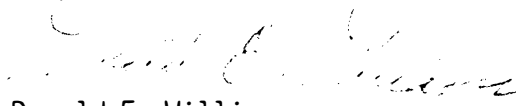
Donald E. Williams
Commissioner

Mail Address
P.O. Box 27412
Richmond, Virginia 23269

TO THE GENERAL ASSEMBLY OF VIRGINIA

There is transmitted herewith the report from the Division of Motor Vehicles required by House Joint Resolution No. 231, Session of 1981, requesting the Division of Motor Vehicles and Department of State Police to evaluate the feasibility of requiring a thumbprint on drivers' licenses and identification cards.

Respectfully submitted,


Donald E. Williams
Commissioner



A Partnership With the Public

STUDY TASK FORCE

Division of Motor Vehicles

- J. C. Skelton, Administrator
Investigative Services
- J. L. Hazelwood, Jr., Administrator
Field Services
- G. L. White, Jr., Administrator
Driver Services
- J. C. Chandler, Jr., Chief
Hearings Office
- Ann F. Ober, Director
Public Information Office

Department of State Police

- Lt. Edward E. Schneider
Assistant Records and Statistics Officer

Division of Consolidated Laboratories

- John W. Tyler, Forensic Scientist
(Fingerprint Expert)

Department of Management Analysis and Systems Development

- Alan Barnes, Program Manager
Criminal Justice Information Systems
- Elaine Zacharias, Project Leader
Criminal Justice Information Systems

Business Community

- Seale A. Moorer, Owner and Secretary
The Imp Pedlar
1806 East Belt Boulevard
Richmond, Virginia
Chairman of the Board of Directors
Retail Merchants Association of Greater Richmond

HOUSE JOINT RESOLUTION NO. 231

Requesting the Division of Motor Vehicles and Department of State Police to evaluate the feasibility of requiring a thumbprint on drivers' licenses and identification cards.

Patrons-Barry, Dillard, and Callahan

Referred to the Committee on Roads and Internal Navigation

WHEREAS, the Division of Motor Vehicles provides identification cards as well as drivers' licenses to citizens of this Commonwealth; and

WHEREAS, in our modern society these credentials are becoming increasingly vital as a method of identification for credit and other monetary purposes; and

WHEREAS, the misrepresentation of persons applying for these sources of identification has proliferated and, at present, there is no viable way to eliminate such misrepresentation; and

WHEREAS, the fraudulent use of such credentials is costing our society vast sums of money each year; and

WHEREAS, the requiring of a thumbprint on a license or identification card would be an additional step in the attempt to provide a valid, single credential which can be safely used as a method of owner verification; now, therefore, be it

RESOLVED by the House of Delegates, the Senate concurring, that the Division of Motor Vehicles and the Department of State Police are hereby requested to evaluate the feasibility of requiring a thumbprint on drivers' licenses and identification cards issued by the Division and make its recommendations to the General Assembly prior to the nineteen hundred eighty-two session.

Table of Contents

| | PAGE |
|---|------|
| I. Summary of Findings. | 1 |
| II. Problems with Current Drivers' Licenses and Identification Cards | 4 |
| III. Constraints/Considerations | 6 |
| IV. Proposed Solution. | 7 |
| Description | 7 |
| Benefits. | 8 |
| Funding Considerations. | 9 |
| Recommended Action. | 10 |

I. SUMMARY OF FINDINGS

Our feasibility study indicated that:

- ° Annual losses to United States businesses due to false identification credentials amount to between 10 and 15 billion dollars. Annual losses in Virginia are at least proportionate to this national figure.
- ° Business losses due to fraudulent use of identification credentials are passed on to all consumers, substantially increasing the cost of living for the citizens of Virginia.
- ° Governmental agencies also experience losses through the use of false identification such as unemployment compensation fraud and multiple welfare payments. Law enforcement agencies encounter problems in establishing the true identity of a suspect due to the ease of establishing and supporting an alias.
- ° Virtually every citizen of Virginia uses some form of personal identity verification documentation, the most common form being the driver's license. Credit cards are the second most common identity credential, followed by social security and military identification cards.
- ° Businesses assume that state-issued identity verification credentials are inherently valid. This assumption is incorrect, because the Commonwealth of Virginia currently has no practical method by which to validate the truth of an applicant's assertion of personal identity.
- ° Even if an identity document is issued to the right person, there is no foolproof method to prevent its later unauthorized use by another person. Although there is usually some form of personal description information on the credential, verification by personal features description can be defeated by a variety of means.
- ° Two basic problems must therefore be resolved: first, to establish a means of increasing the integrity and security of the initial identity documentation authorization process; second, to provide a reliable means of validating individual instances of identity verification in the field.

A fingerprint verification system would help to solve the first problem by preventing a person who already had a license from obtaining others under different names. However the greatest benefit of such a system would be in solving the second problem; ensuring that the person using a license was the one to whom it had been issued.

Proposed Solution

- ° Several methods of fingerprint verification processing are available, including simple manual visual comparison and certain advanced forms of automated fingerprint matching techniques. We immediately rejected manual visual comparison because of the practical difficulties associated with making field verifications on this basis.
- ° A preliminary review of technical literature on the subject indicates that a number of automated fingerprint matching systems exist which might effectively resolve the problem of securing a reliable means to validate personal identity in the field. These systems are now in an advanced state of development and are oriented toward both commercial and governmental identity verification procedures.

Recommendation

- ° We conclude that it is possible with current technology to develop a reliable method of personal identity verification by means of an automated finger image verification system. This technology could be designed to be compatible with both government and commercial applications. We believe that the adoption of such a means of positive personal identity verification could save substantial sums of money now lost due to the fraudulent use of drivers' licenses and identification cards. We propose that a study be performed to determine the costs and benefits of such a system for the Commonwealth of Virginia.

NOTE: It has been stated that the fraudulent use of drivers' licenses occurs in two areas: (1) illegally obtained drivers' licenses that are reflective of the career criminal element; and (2) unauthorized use of a driver's license. This unauthorized use ranges in scope from stolen licenses used for criminal aliases or bad checks to the lending of a license to a minor in order to purchase of alcoholic beverages.

In regard to the first area, the Division of Motor Vehicles feels that it is presently doing all that is legally possible in order to ensure

true identity when applying for a license. However, the implementation of such a system should have a deterrent effect on this problem in that criminals would tend to avoid any process in which their finger images would be utilized.

The second area, unauthorized use, would be the primary target of the proposed system. The system should almost totally eliminate this area of fraud. This would be due to the fact that the true owner of a license would have to be physically present in order for positive/ approved identity verification.

Through these methods, the scope of fraud should be reduced dramatically.

II. PROBLEMS WITH CURRENT DRIVERS' LICENSES AND IDENTIFICATION CARDS

Since almost every adult citizen of the Commonwealth of Virginia uses a driver's license or identification card as an identity verification credential, such documents have become increasingly necessary as our society becomes more reliant on cashless transactions. This reliance on these credentials has resulted in an increase in the use of drivers' licenses and identification cards for fraudulent purposes.

Of all types of personal identity documentation, drivers' licenses are used more often than any other type as an accepted means of positively identifying individuals in commercial and legal applications. The second most commonly used identity document is the credit card, followed by social security and military identification cards.

Common usage of the driver's license as the primary identification document has led to the twin assumptions that these credentials are secure (that is, that the information contained on them is correct) and that they are being used by the same person whose identity they describe. Neither assumption is inherently correct. Abuses can and do occur in the application process, and drivers' licenses are frequently obtained and used to fraudulently obtain cash or merchandise.

Illegally Obtained Drivers' Licenses

Current procedures for driver's license issuance in Virginia depend to a large extent on the veracity of the individual applying for these credentials. No practical or reasonable means exists to independently verify alleged identities of applicants.

Unauthorized Use Of Drivers' Licenses

Once issued, verification of personal identity through the use of information printed on the driver's license depends on the skills and ability of the individual making the verification attempt. If this person is careless, or if the person using the license resembles the true licensee, attempted fraudulent use of the license will not be detected.

Because a positive identification on the basis of a subjective examination and comparison of personal description or photographic likeness information is normally difficult for most persons, the potential for fraud is not substantially reduced by including such information on identity documents.

Commercial Problems

Nearly 80 percent of all commercial losses in the United States are due to non-violent actions, including paper

transactions. According to the American Management Association, "paper crimes" accounted for approximately \$40 billion in losses during 1980. Of this amount, between \$10 and \$15 billion were lost in transactions where false identification documents played a primary role. These losses are passed on indirectly to consumers, raising the cost of living for everyone. The annual share of consumer fraud costs for every Virginia citizen was \$165, or approximately \$821,700,000 statewide. Of this overall statewide fraud loss, more than \$200 million was due to fraud involving false identification.

A solution to many forms of "paper crime" problems lies in the ability to safeguard the integrity and reliability of personal identity verification documents, especially the driver's license. In view of the reliance placed on this form of identify credential by commercial interest, it also appears that a satisfactory solution to the problem of identity credentials fraud must involve a method of ad hoc field verification; that is, a method which can be utilized by merchants and other in the daily business of verifying personal identities in a variety of transactions and situations.

Government Problems

Certain governmental interests also apply to the problem of establishing a means of personal identity verification. The use of false identity documentation reduces the likelihood of appropriate governmental control in situations such as voting and motor vehicle operation.

False drivers' licenses may be used to perpetrate welfare and unemployment compensation fraud, and to cash stolen government benefit checks. They may also be used by wanted criminals to establish false identities and evade detection and apprehension by the police.

III. CONSTRAINTS/CONSIDERATIONS

Certain practical and legal concerns should be considered with regard to the application of finger image identification technology in personal identity verification.

The first concern is the matter of technical capability. While it appears that several technological solutions to the problem of finger image recognition and matching exist, no such solution has ever been applied to the precise question posed by Resolution No. 231, however, we understand that several commercial firms are developing systems capable of meeting the requirement of a personal identification system based on finger image matching using standardized documents such as drivers' licenses, but that currently no system is available for immediate testing against this application. The reason for this appears to be that no demand has yet been made on the developers to solve this problem.

The second problem is one of affordable cost. The final system must be capable of independent remote operations. Individual units must be priced low enough to be affordable by all levels of the business community.

The third area is legal. There should be no problem with amending the motor vehicle code setting forth the procedure for obtaining a license to require the taking of a finger image. The Division of Motor Vehicles would use the finger image to determine if the applicant had made a false statement in the application or had been convicted of a motor vehicle offense that would disqualify him from obtaining a license. Beyond that, any government agency or private party using the system, would simply have it as a tool to determine if a proffered driver's license belonged to the person possessing it.

IV. PROPOSED SOLUTION

Description

Law enforcement operations routinely use fingerprints to establish the positive identity of persons arrested for criminal offenses. These manual fingerprint identification systems require trained experts to individually examine fingerprint records and compare them in order to identify matches with known fingerprint files, however, manual techniques such as those used by law enforcement fingerprint examiners do not appear to be feasible for commercial applications. Such techniques require a level of expertise on the part of the examiner which is not available at normal levels of commercial operations. Merely recording a fingerprint on a driver's license therefore does not appear to be a feasible solution to the overall problem of personal identity credentials verification.

Systems exist which are capable of automatically enrolling, reading and matching a finger image against a known file of finger image records previously recorded. Such systems utilize various sophisticated, computerised algorithms to identify differences among finger images and to rapidly scan recorded sets of authorized finger image records in order to accomplish personal identity verification.

We propose that the General Assembly consider the implementation of this type of automated finger image identification system which could be made a part of the Virginia drivers' licenses and identification cards. This system would use electronic means to automatically enroll license applicants and to encode finger image data on the driver's license and identification card. Direct field matching could then be performed by remote sensing terminals designed to scan the individual's finger image and to compare such data against that embedded in the driver's license or the identification card.

Before the issuance of a driver's license or identification card, the Division of Motor Vehicles would require proof of identity, and direct the applicant to place a finger on a platen linked to a scanning device which then digitizes the finger image and converts this data to an electronic code.

This electronically coded finger image information is then encrypted and stored on the individual applicant's driver's license or identification card by means of a magnetic strip, an embedded microchip, or some other form of secure data storage medium. The rest of the license or identification card would be prepared in the normal way and issued to the applicant.

Prior to implementing the system, the Division of Motor Vehicles would publish and distribute a description of the standard requirements necessary to read and compare finger

images against the data stored on drivers' licenses or identification cards. On the basis of these standards, commercial interests could then compete to provide low cost hardware systems capable of utilizing the fingerprint data stored on licenses and identification cards to validate personal identity at the point of sale or transaction.

Commercial Uses

The remote finger image comparison systems would provide businesses the capability of checking the identification of a person using a credit card, cashing a check or returning merchandise. These systems would verify whether a person matches the driver's license or identification card. This capability would have a significant impact on the unauthorized use of credit cards or checks.

Government Use

The Division of Motor Vehicles would have the capability of checking for duplicate licenses at time of issuance. This would eliminate one person having multiple drivers' licenses in different names.

Governmental agencies such as the Department of Welfare could use the remote systems to compare finger images on site to verify identities.

Benefits

Public service systems have the potential for both quantifiable and nonquantifiable benefits. Certainly, there is an enormous potential for quantifiable benefits due to reductions in fraud attributable to false identification.

For example, if we prorate a conservative national estimate of \$10 billion dollars lost annually to fraud involving false identification against the current population of Virginia, we see that the potential for savings on this basis alone is in excess of \$200 million each year.

In addition, certain nonquantifiable benefits are likely to accrue as a consequence of implementing a more secure means of personal identification. The encoded finger image on a driver's license will have a marked deterrent effect on illegal acquisition of drivers' licenses and identification cards. For example, making the method of personal identification more reliable will surely streamline the process of paper transactions based on personal identity information. It should be easier to cash checks and to establish and use credit where commercial interests are more confident of the integrity of the identification process.

A reduction in business costs attributable to fraud - costs which are normally passed on to all consumers - should be reflected in lower overall consumer costs.

Other governmental agencies will also benefit, such as:

- State Medical Examiner (finger images will aid the identification of deceased persons)
- Alcoholic Beverage Commission (proof of age in ABC stores and commercial establishments)
- State Employment Commission (reduce unemployment compensation fraud)
- Welfare (identification of applicants and reduction of multiple benefit payments)
- Immigration (field identification validation)

Funding Consideration

Implementation of a system of personal identification based on finger image data stored on drivers' licenses and identification cards will require that the Commonwealth purchase an encoding system for embedding finger image data on drivers' licenses and identification cards and a series of reading/comparison terminals for all state agencies desiring to use the system.

Commercial interests desiring to use the system will have to acquire reading/comparison terminals capable of decoding the finger image data embedded in the license and identification card and comparing this data against the finger images of customers taken at the point of transaction. We believe that current developments in this area will result in terminal costs which are commercially feasible.

We believe that further development of this concept should be funded in three logical phases:

- Phase One: Cost Benefit Study (to define system requirements and prepare preliminary system design, determine operational and development costs, conduct engineering surveys to determine hardware costs, and conduct user surveys of both governmental and commercial users to determine benefits)
- Phase Two: Systems Analysis and Development (to prepare system design and negotiate purchase of the system)
- Phase Three: Implementation

We believe that Phase One could be completed by the Division of Motor Vehicles for an amount not to exceed \$50,000; Phase Two and Three costs will be estimated during this initial effort. Phase One should take approximately nine months to complete after funds are appropriated.

Funding for commercial applications would be entirely the responsibility of the private sector. Since the primary beneficiary of the system will be retail commercial interests, we believe that it is appropriate to develop this concept in conjunction with retail merchants associations and to discuss the potential for deferring a portion of the state system development and implementation costs to them.

Alternatively, the state could offset some of its cost of acquiring and supporting the system by licensing the remote point of sale units.

Recommended Action

We recommend that the General Assembly appoint a Steering Committee organized through the Division of Motor Vehicles to initiate a cost benefit study concerning the feasibility of utilizing automated finger image devices as a means of personal identity verification for those who possess a driver's license or identification card issued by the Division of Motor Vehicles.

The expertise necessary to conduct such a study is available through the Department of Management Analysis and Systems Development. Therefore we recommend that the Steering Committee, as proponent of the system, appoint MASD as the technical advisor for the cost benefit study.

The results of this study will provide the General Assembly with a clear picture of all expected costs and benefits attributable to the implementation of an automated personal identity verification system.

