

**GIBBONS DEL DEO, DOLAN,  
GRIFFINGER & VECCHIONE, P.C.**  
One Riverfront Plaza  
Newark, New Jersey 07102-5497  
(973) 596-4729 (phone)  
(973) 639-6279 (fax)

★ FEB 20 2003 ★

LONG ISLAND OFFICE

**CV 03 0825**

**PLATT, J.  
ORENSTEIN, M.**

One Pennsylvania Plaza, 37th Floor  
New York, New York 10119  
(212) 649-4700

Kevin J. McKenna (KM 7530)  
Vincent E. McGearry (VM 1742)

(S.I.)

*Attorneys for Plaintiff  
Intelli-Check, Inc.*

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

INTELLI-CHECK, INC.,

Plaintiff,

v.

CARDCOM TECHNOLOGY, INC.,

Defendant.

Civil Action No.

**COMPLAINT  
AND  
JURY DEMAND**

Plaintiff Intelli-Check, Inc. ("Plaintiff Intelli-Check"), by and through its counsel,  
Gibbons, Del Deo, Dolan, Griffinger & Vecchione, a Professional Corporation, brings this action  
for patent infringement and avers as follows:

## **PARTIES**

1. Plaintiff Intelli-Check is a corporation duly organized and existing under the laws of the State of Delaware, with its principal place of business at 246 Crossways Park West, Woodbury, New York 11797.

2. Upon information and belief, Defendant CardCom Technology, Inc. ("Defendant CardCom"), is a corporation organized and existing under the laws of the State of California with a regular and established place of business at 6301 Beach Boulevard, Suite 216, Buena Park, California 90621.

## **JURISDICTION AND VENUE**

3. This Court has subject matter jurisdiction pursuant to the provisions of 28 U.S.C. §§ 1331 and 1338(a).

4. Venue is proper in this District pursuant to the provisions of 28 U.S.C. §§ 1400(b) and 1391(b)(2) because, upon information and belief, Defendant CardCom has committed acts of infringement in this District including, but not limited to, making, having made, using, causing others to use, selling and marketing patented methods, products and systems in and to the District.

## **BACKGROUND**

5. Plaintiff Intelli-Check is the owner by assignment of all right, title and interest in and to United States Patent No. 6,463,416 B1 (the "'416 Patent") for "Authentication System For Identification Documents," which was duly and lawfully issued by the United States Patent and Trademark Office to Plaintiff Intelli-Check on October 8, 2002. A copy of the '416 Patent is attached hereto as Exhibit A.

6. Upon information and belief, Defendant CardCom makes, uses and sells automated age verification systems, one of which systems is referred to as the "Viage" system.

**COUNT ONE-PATENT INFRINGEMENT**

7. Plaintiff Intelli-Check repeats and realleges each and every allegation contained in paragraphs 1 through 6 as if fully set forth herein.

8. Upon information and belief, Defendant CardCom's automated age verification systems, including but not limited to the "Viage" system, infringe one or more of the claims of the '416 Patent.

9. Plaintiff Intelli-Check did not at anytime authorize Defendant CardCom to make, have made, use or sell any method, product or system covered by the '416 Patent.

10. Upon information and belief, Defendant CardCom is infringing the '416 Patent by making, having made, using, causing others to use and selling its automated age verification systems.

11. By reason of infringement of the '416 Patent, Plaintiff Intelli-Check has been irreparably harmed and is entitled to the remedies provided under the United States patent laws.

**COUNT TWO-INDUCEMENT TO INFRINGE**

12. Plaintiff Intelli-Check repeats and realleges each and every allegation contained in paragraphs 1 through 11 as if fully set forth herein.


13. Upon information and belief, at all material times herein, Defendant CardCom has advertised, marketed, offered for sale and sold to its customers infringing automated age verification systems.

14. Upon information and belief, Defendant CardCom has knowingly and willfully aided and abetted, induced, and directed its customers to infringe upon the '416 Patent, in violation of 35 U.S.C. § 271(b).

**WHEREFORE**, Plaintiff Intelli-Check requests judgment in its favor and against Defendant CardCom as follows:

- (a) judgment that Defendant CardCom has infringed the '416 Patent,
- (b) preliminary and permanent injunctive relief prohibiting infringement, inducement of infringement or contributory infringement of the '416 Patent;
- (c) compensatory damages for all activities by Defendant CardCom infringing the '416 Patent;
- (d) prejudgment interest;
- (e) costs of suit and attorneys' fees; and
- (f) such other and further relief as the Court may deem just and appropriate.

**GIBBONS, DEL DEO, DOLAN,  
GRIFFINGER & VECCHIONE, P.C.**  
One Pennsylvania Plaza, 37th Floor  
New York, New York 10119

By:   
Kevin J. McKenna (KM 7530)  
Vincent E. McGeary (VM 1742)  
*Attorneys for Plaintiff*  
*Intelli-Check, Inc.*

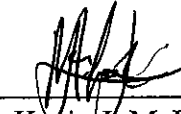
Dated: February 19, 2003  
New York, New York

**DEMAND FOR A JURY TRIAL**

Pursuant to Rule 38(b), Plaintiff Intelli-Check hereby demands a trial by jury on all issues so triable.

**GIBBONS, DEL DEO, DOLAN,  
GRIFFINGER & VECCHIONE, P.C.**  
One Pennsylvania Plaza, 37th Floor  
New York, New York 10119

By: \_\_\_\_\_



Kevin J. McKenna (KM 7530)  
Vincent E. McGeary (VM 1742)  
*Attorneys for Plaintiff  
Intelli-Check, Inc.*

Dated: February 19, 2003  
New York, New York

Exhibit A



US006463416B1

(12) **United States Patent**  
Messina

(10) Patent No.: **US 6,463,416 B1**  
(45) Date of Patent: **\*Oct. 8, 2002**

(54) **AUTHENTICATION SYSTEM FOR IDENTIFICATION DOCUMENTS**

(75) Inventor: **Kevin M. Messina**, Huntington, NY (US)

(73) Assignee: **Intelli-Check, Inc.**, Woodbury, NY (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/236,531**

(22) Filed: **Jan. 25, 1999**

**Related U.S. Application Data**

(63) Continuation of application No. 08/680,452, filed on Jul. 15, 1996, now Pat. No. 5,864,623.

(51) Int. Cl.<sup>7</sup> ..... **G06F 17/60**

(52) U.S. Cl. .... **705/1; 235/380; 340/5.86; 902/5; 382/12; 382/13; 382/115; 707/505; 707/506; 707/508**

(58) Field of Search ..... **235/375, 380, 235/487, 488, 442; 380/23, 51; 705/1; 707/505, 506, 508; 283/83, 904; 340/5.86; 902/5; 713/179; 382/12, 13, 115; 714/771**

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

3,569,619 A 3/1971 Simjian  
3,868,057 A 2/1975 Chavez  
3,906,201 A 9/1975 Housman et al.

(List continued on next page.)

**FOREIGN PATENT DOCUMENTS**

CH 1546053 5/1979  
DE 2802430 7/1978  
DE 3050473 9/1986  
DE 4410459 2/1995

DE 19527737 2/1996  
EP 0187448 1/1991  
EP WO009412372 \* 6/1994  
EP 0683471 11/1996  
FR 2571873 10/1986  
GB 2067322 7/1981  
GB 2136180 9/1984  
JP 0050075879 3/1993  
JP 0080101868 4/1996

**OTHER PUBLICATIONS**

New auto-entry rules don't make crossing any easier, Lazaro Leon, Apr. 1993.\*

Software licence agreements in Spain, Ulloa Gonzal, 04, 1993.\*

Natural Language, Work-Group Computing Report, Jan. 1992.\*

On The Horizon, Barry Gerber, Network Computing, 1995.\*

IBM OS-2 with graphic interface, Electronic News, Nov. 1988.\*

Best Practices Recommendations For the use of Magnetic Stripes, by AAMVA, Apr. 1996.\*

TX-4-024-478 "ID-Check Source Code Listing" Dec. 12, 1994.

TX-4-024-479 "ID-Check Source Code Listing" Jul. 10, 1995.

Best Practices Recommendations For The Use Of Magnetic Stripes, Version 2.0, Apr. 1996 by AAMVA (The American Association of Motor Vehicle Administrators).

Primary Examiner—Eric W. Stamber

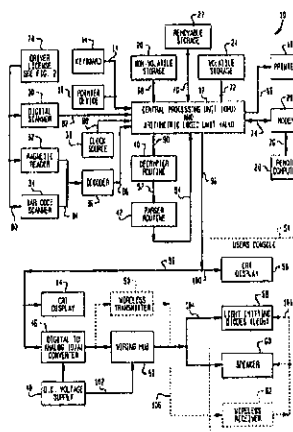
Assistant Examiner—Mussie Tesfamariam

(74) Attorney, Agent, or Firm—Gibbons, Del Deo, Dolan, Griffinger & Vecchione

(57) **ABSTRACT**

A programming apparatus that authenticates the contents of driver licenses having both human recognizable information and machine readable information is disclosed. The contents of the driver licenses are verified without encountering any human error. The verified contents of the driver licenses may be transferred to a remote computer for other identification purposes such as preordained organ donors or possible criminal prosecution.

**29 Claims, 7 Drawing Sheets**



## US 6,463,416 B1

Page 2

## U.S. PATENT DOCUMENTS

3,956,615 A	5/1976	Anderson et al.	5,336,871 A	8/1994	Colgate, Jr.	
4,138,057 A	2/1979	Atalla	5,337,358 A	8/1994	Axelrod et al.	
4,193,131 A	3/1980	Lennon et al.	5,341,428 A	8/1994	Schatz	
4,304,961 A	12/1981	Campbell, Jr.	5,422,468 A	6/1995	Abecassis	
4,357,529 A	11/1982	Atalla	5,453,600 A	9/1995	Swartz	
4,450,348 A	5/1984	Stockburger et al.	5,490,217 A	2/1996	Wang et al.	
4,453,074 A	6/1984	Weinstein	5,500,518 A	3/1996	Olzak et al.	
4,471,216 A	9/1984	Herve	5,513,261 A	4/1996	Maher	
4,629,872 A	12/1986	Hällberg	5,514,860 A	5/1996	Berson	
4,659,914 A	4/1987	Kondo et al.	5,546,278 A	8/1996	Bethurum	
4,752,676 A	6/1988	Leonard et al.	5,553,143 A	9/1996	Ross et al.	
4,807,287 A	2/1989	Tucker et al.	5,590,193 A	12/1996	Le Roux	
4,811,393 A	3/1989	Hazard	5,651,066 A	7/1997	Moriyasu et al.	
4,811,408 A	3/1989	Goldman	5,661,805 A	8/1997	Miyauchi	
4,816,657 A	3/1989	Stockburger et al.	5,663,553 A	9/1997	Aucsmith	
4,879,747 A	11/1989	Leighton et al.	5,679,940 A	10/1997	Templeton et al.	
4,993,068 A	2/1991	Plosenka et al.	5,694,471 A	12/1997	Chen et al.	
5,007,089 A	4/1991	Matyas et al.	5,712,472 A	1/1998	Lee	
5,140,634 A	8/1992	Guillon et al.	5,721,777 A	2/1998	Blaze	
5,163,098 A	11/1992	Dabhura	5,770,084 A	6/1998	Novis et al.	
5,237,611 A	8/1993	Rasmussen et al.	5,786,587 A	7/1998	Colgate, Jr.	
5,249,227 A	9/1993	Bergum et al.	5,812,664 A	9/1998	Bernobitch et al.	
5,259,025 A	11/1993	Monroe et al.	5,848,426 A	* 12/1998	Wang et al.	707/505
5,267,315 A	11/1993	Narita et al.	5,864,623 A	* 1/1999	Messina et al.	380/23
5,321,751 A	6/1994	Ray et al.				

\* cited by examiner



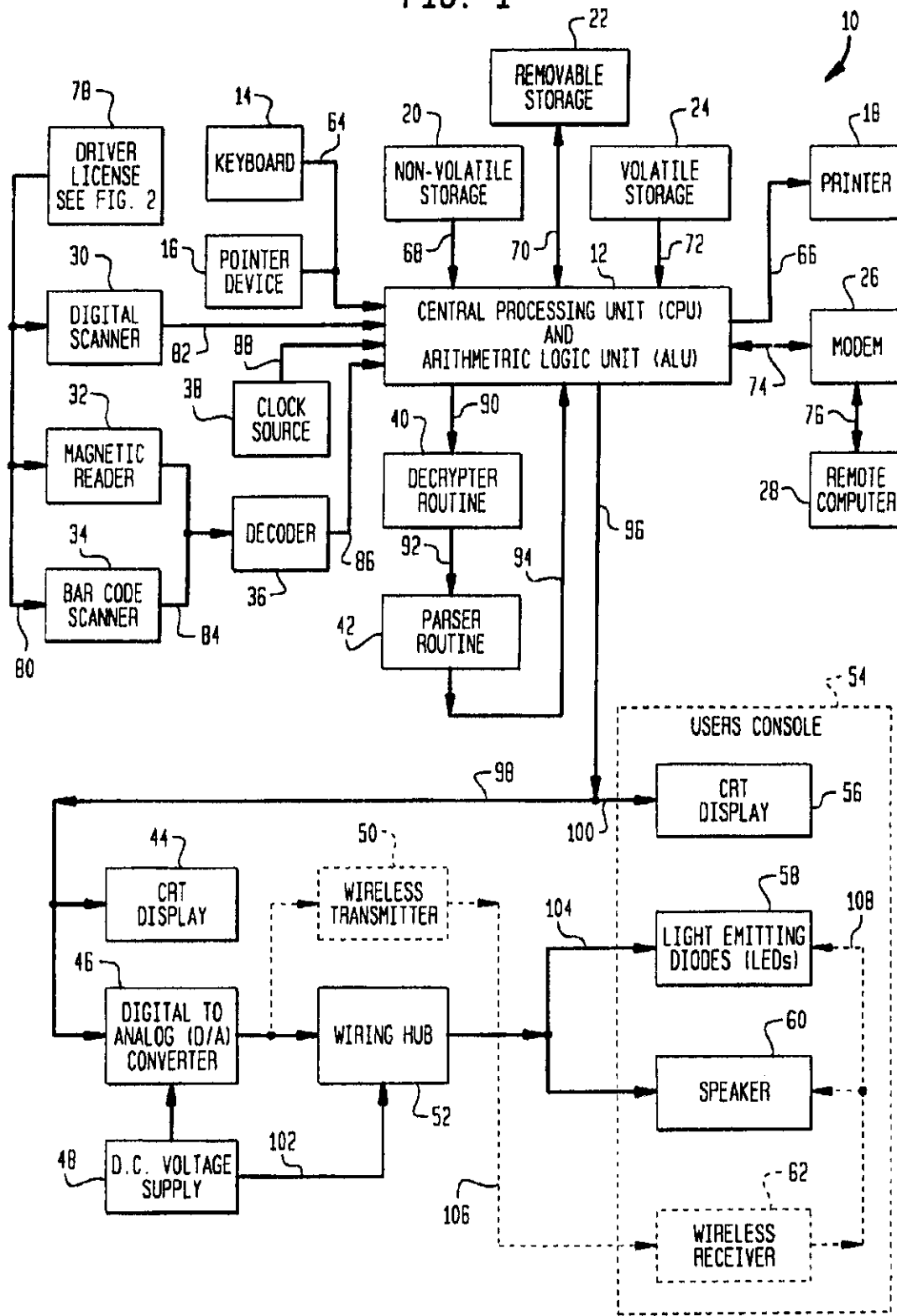
U.S. Patent

Oct. 8, 2002

Sheet 1 of 7

US 6,463,416 B1

FIG. 1



U.S. Patent

Oct. 8, 2002

Sheet 2 of 7

US 6,463,416 B1

FIG. 2A

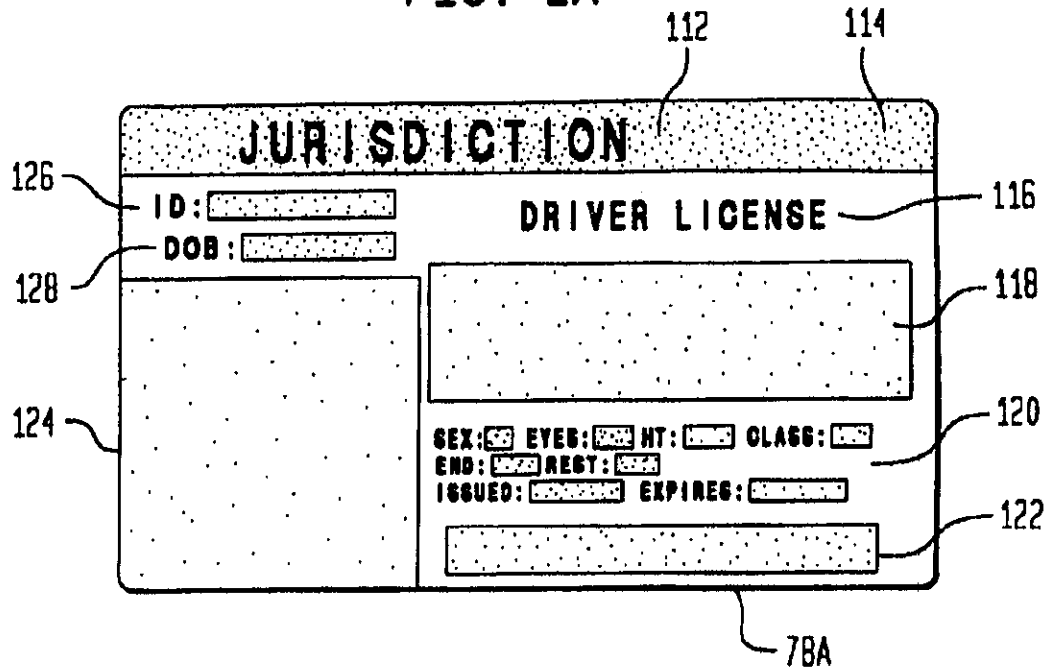
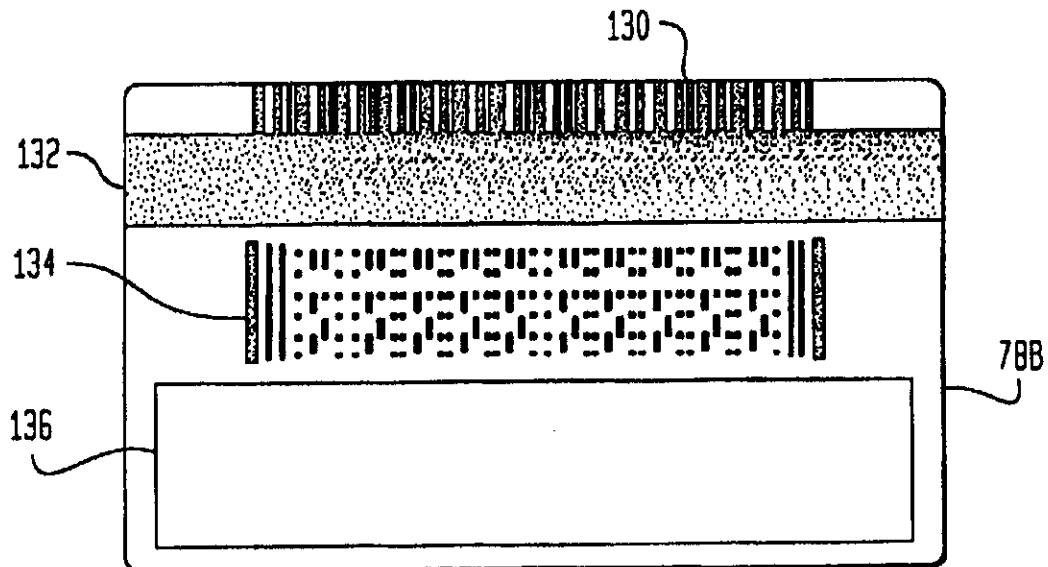


FIG. 2B

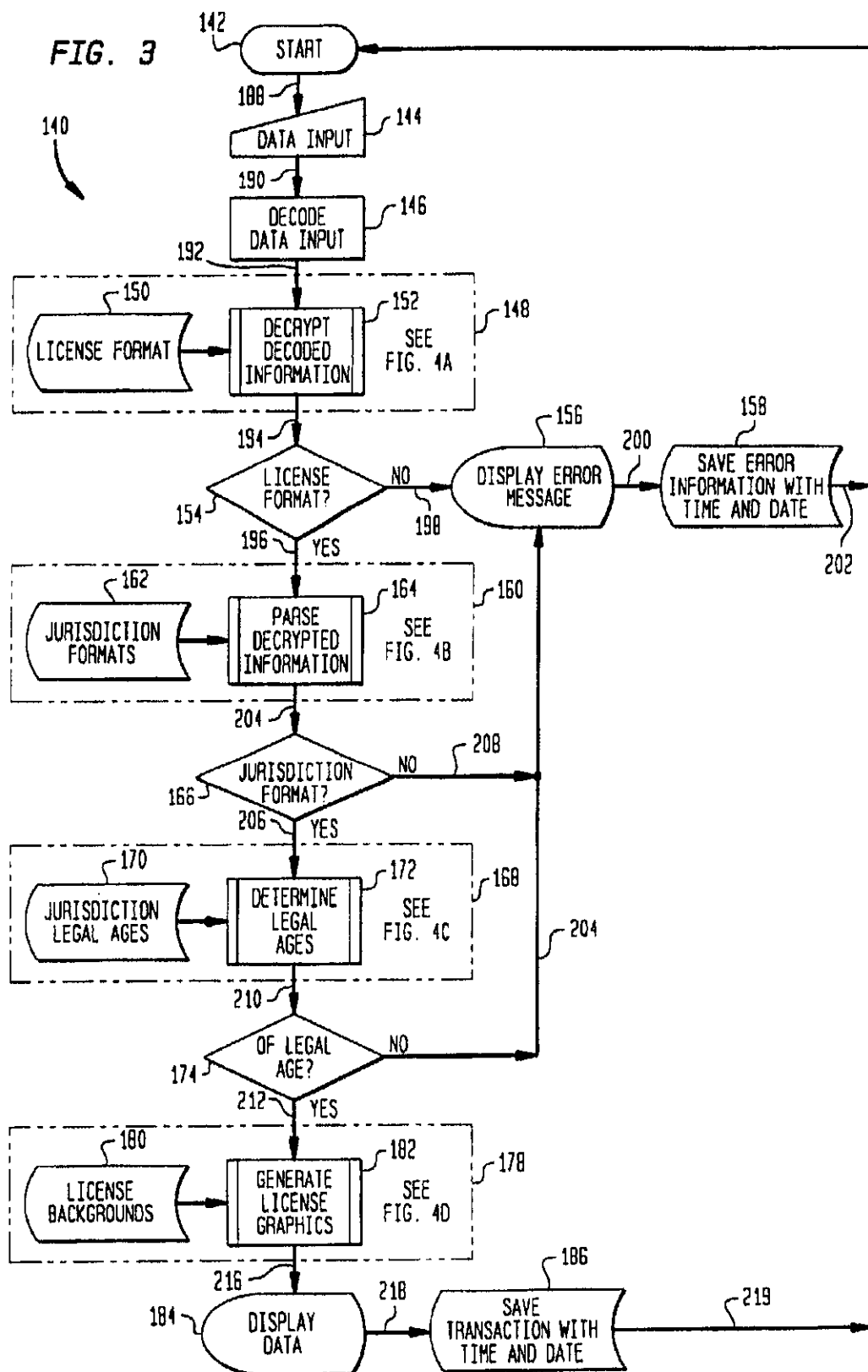


U.S. Patent

Oct. 8, 2002

Sheet 3 of 7

US 6,463,416 B1

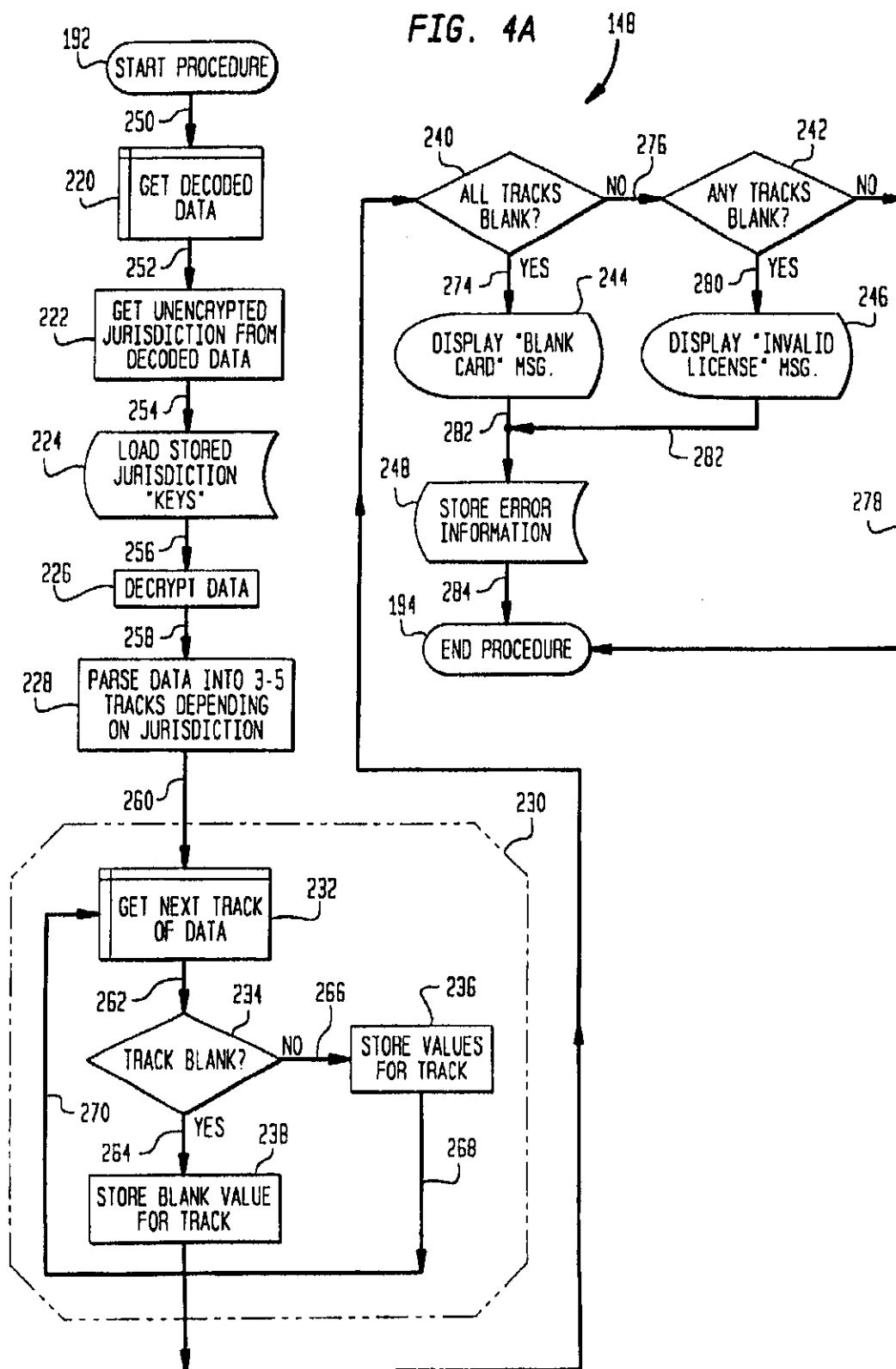


U.S. Patent

Oct. 8, 2002

Sheet 4 of 7

US 6,463,416 B1

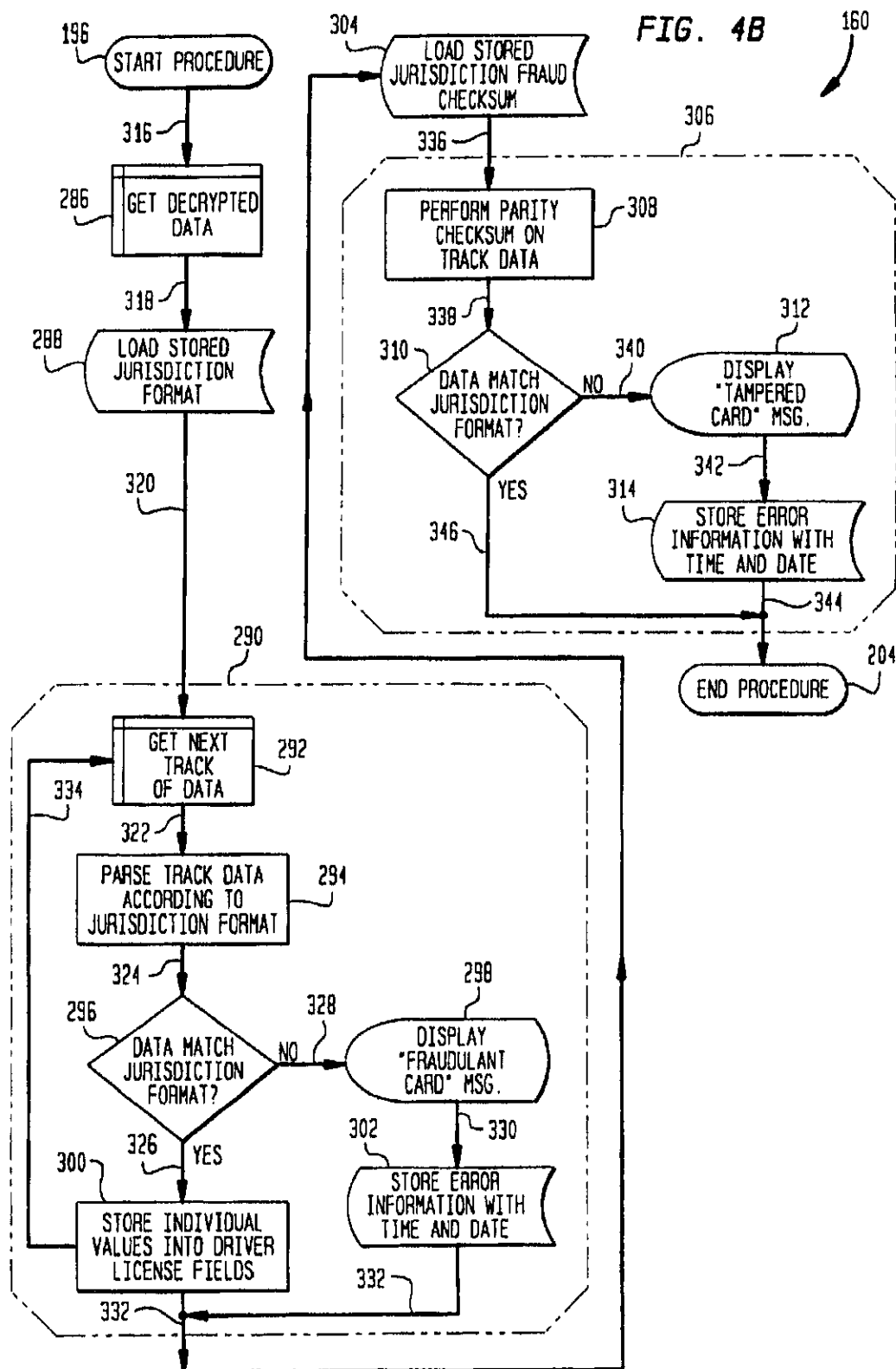


U.S. Patent

Oct. 8, 2002

Sheet 5 of 7

US 6,463,416 B1

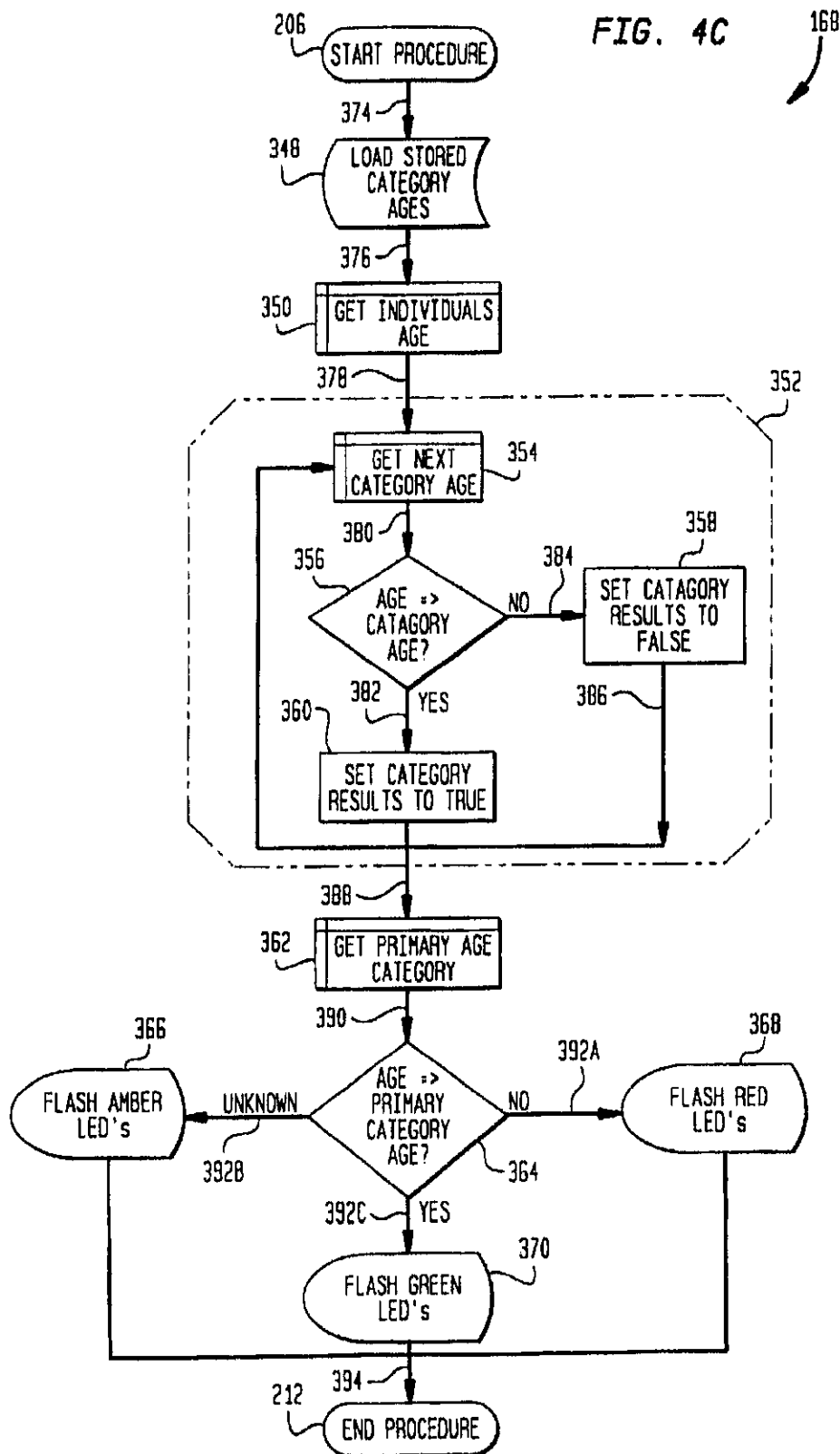


U.S. Patent

Oct. 8, 2002

Sheet 6 of 7

US 6,463,416 B1



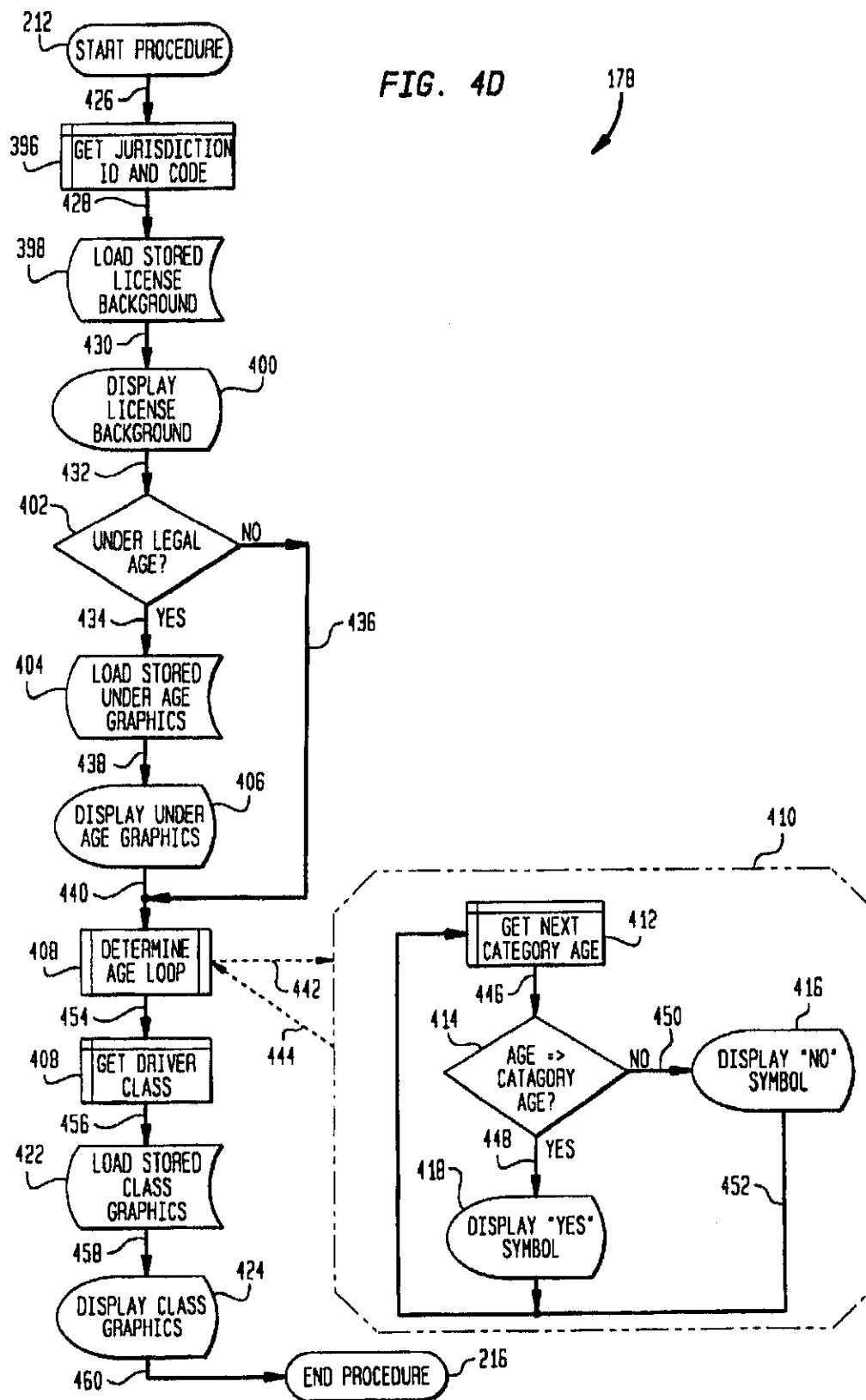
U.S. Patent

Oct. 8, 2002

Sheet 7 of 7

US 6,463,416 B1

FIG. 4D



US 6,463,416 B1

1

**AUTHENTICATION SYSTEM FOR  
IDENTIFICATION DOCUMENTS****Cross Reference to Related Application**

This application is a continuation of application Ser. No. 08/680,452 filed on Jul. 15, 1996, now U.S. Pat. No. 5,864,623 which is incorporated herein by reference.

**BACKGROUND OF THE INVENTION****1. Field of the Invention**

The present invention generally relates to an identification system for documents. More particularly, the present invention relates to a programmable apparatus for authenticating drivers' licenses used for identification purposes. Specifically, the present invention relates to a programmable apparatus that identifies the contents of the driver licenses used for identification purposes without any human error and allows the information carried by the driver licenses to be transferred to a remote location for further identification purposes.

**2. Description of Related Art**

The problem of rampant and readily available fake identification cards, more particularly, driver licenses/identification cards, has caused many retailers fines, sometimes imprisonment, loss of tobacco and liquor licenses, and has even subjected them to other forms of civil and criminal liability. Over the course of years, various attempts have been made to prevent or detect the use of fake identification cards, but not with a great deal of success. To help prevent the use of fake identification, since 1992 the United States and Canada have been issuing new driver licenses in accordance with an international North American Free Trade Agreement (NAFTA) standard created and enforced by the American Association of Motor Vehicle Administrators (AAMVA). These new driver licenses/identification cards have embedded coded, or even encrypted coded information, with machine readable formats that conform to the NAFTA standards. It is desired that means be provided that authenticate the contents of these identification cards so as to safeguard the retailer against the penalties that may otherwise be encountered by fake identification cards.

The use of driver licenses has expanded over the years to serve as identification for various applications, such as for the purchase of alcohol, tobacco or lottery products, as well as for gambling in casinos, off-track betting (OTB), movie theaters and user-definable events, such as allowing the ingress into liquor establishments. All of these fields have an age requirement for the purchase of a product at the point-of-transaction or for ingress into an establishment and the driver license is the document used to provide age identification and all age verification is commonly accomplished in a relatively quick manner. It is desired that means be provided that easily decides a driver licenses authenticity so that any purchase of a product having an age requirement is satisfied at the time of purchase and in a quick and convenient manner.

As is known, driver licenses are accompanied with photo identification of the particular driver, and in addition to the identification supplied by a driver's license to a liquor retailer, the driver license is frequently used for other identification purposes, such as for providing proper identification for check cashing. The frequent use of driver licenses allows the licenses to serve as tools to detect or uncover individuals who are being sought out because of being subject to pending criminal prosecution. It is desired

2

that means be provided to allow the information on the driver licenses to be transferred to a local or remote jurisdiction to help identify and detect individuals that may be classified as being offenders against the criminal law of the associated jurisdiction.

Driver licenses not only serve for identification for commercial transactions, but also serve a humanitarian need of identifying preordained organ donors that may be involved in tragic accidents. It is desired for humanitarian purposes that means be provided to transfer the organ donor information commonly present on driver licenses to a local or remote jurisdiction so that an available organ donor may be quickly matched to an individual in need of the now-available organ.

Driver licenses are commonly used in places of business, such as convenience stores, liquor stores, entertainment centers which also have personal computers for use in business purposes, such as inventory management. It is desired that means be provided so that personal computers may be readily adapted to serve as an integral part of an authentication system for driver licenses.

**OBJECTS OF THE INVENTION**

It is a primary object of the present invention to provide an authentication system to authenticate driver licenses that are coded with machine readable information conforming to AAMVA standards.

It is a further object of the present invention to provide an authentication system for not only verifying the contents of a driver license, but also allowing for the information to be transferred to a local or remote jurisdiction so that it may be identified for criminal prosecution purposes or, conversely, for humanitarian purposes, such as for identifying preordained organ donors.

It is another object of the present invention to provide an identification system that utilizes personal computers that are commonly found in places of business having a need for authenticating the contents of a driver license used for identification purposes.

**SUMMARY OF THE INVENTION**

The present invention is directed to an authentication system that verifies the contents of documents, such as driver licenses.

The authentication system comprises a programmable apparatus that verifies the contents of the document embodying both human recognizable information and machine recognizable coded information. The apparatus comprises means for reading, means for parsing, means for comparing and means for displaying. The information of the document is read by the means for reading and directed into the programmable apparatus. The means for parsing reads the information of the document in the programmable apparatus and parses such information into the jurisdictional segments each having predetermined values. The means for comparing analyze the information against the predetermined values and generates a verification signal if the information and the values match. The means for displaying displays the verification signal.

**BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 is a block diagram of the programmable apparatus of the present invention.

FIG. 2 is composed of FIGS. 2(A) and 2(B) that illustrate the human recognizable and machine recognizable formats carried by driver licenses related to the present invention.



US 6,463,416 B1

3

FIG. 3 is a flow diagram of the overall operation of the programmable apparatus.

FIG. 4 is composed of FIGS. 4(A), 4(B), 4(C) and 4(D), that respectively illustrates one of the four (4) primary program subroutines making up the overall operation illustrated in FIG. 3.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to the drawing, wherein the same reference numbers indicate the same elements throughout, there is shown in FIG. 1 a block diagram of a programmable apparatus comprising a computer 12, more particularly, a central processing unit and arithmetic logic unit whose actions are directed by computer programs comprising a series of operational steps performed on information read into the computer 12.

In general, the programmable apparatus authenticates a document embodying information comprising both human recognizable information and machine recognizable information comprising a series of codes. The programmable apparatus comprises means for reading the information of the document into the programmable apparatus, means for parsing the read document information into jurisdictional segments each having predetermined values, and means for comparing the read information of the document against the predetermined values and generating at least a verification signal on a display means, if the information of the document and the predetermined values match. The programmable apparatus comprises a plurality of conventional elements arranged in a non-conventional manner with all elements being listed in Table 1.

TABLE 1

{PRIVATE } REFERENCE NO.	ELEMENT
12	CENTRAL PROCESSING UNIT (CPU) AND ARITHMETIC LOGIC UNIT (ALU)
14	KEYBOARD
16	POINTER DEVICE
18	PRINTER
20	NON-VOLATILE STORAGE
22	REMOVABLE STORAGE
24	VOLATILE STORAGE
26	MODEM
28	REMOTE COMPUTER
30	DIGITAL SCANNER
32	MAGNETIC READER
34	BAR CODE SCANNER
36	DECODER
38	CLOCK SOURCE
40	DECRYPTER ROUTINE
42	PARSER ROUTINE
44	CRT DISPLAY
46	DIGITAL-TO-ANALOG (D/A) CONVERTER
48	D.C. VOLTAGE SUPPLY
50	WIRELESS TRANSMITTER
52	WIRING HUB
54	USER'S CONSOLE
56	CRT DISPLAY
58	LIGHT EMITTING DIODES (LEDS)
60	SPEAKER
62	WIRELESS RECEIVER

The keyboard 14 and the pointer device 16, such as a mouse, provide a means for the operator or user to enter information, via signal path 64, into the CPU 12. The printer 18 converts the outputs, present on signal path 66, of the central processing unit 12 into printed images.

4

The non-volatile storage 20, the removable storage 22, and the volatile storage 24 are all storage mediums, whose contents are controlled and updated by the central processing unit 12, via signal path 68, 70 and 72 respectively. The non-volatile storage 20 and the removable storage 22 provide for permanent recordings of every transaction involved with or determined by the CPU 12, whereas the volatile storage 24 provides temporary storage of information while it is being processed by the CPU 12. The removable storage 22 may be a disk that is insertable and removable from the CPU 12.

The modem 26 is interconnected to the CPU 12 by way of signal path 74 and allows the CPU 12 to share its input and manipulated data, as well as the contents of its storage information, with the remote computer 26, via the signal path 76, which is typically established by a telephone communication link.

The digital scanner 30, magnetic reader 32, and bar code scanner 34 are each capable of reading the information on the identification card 78, to be more fully described with reference to FIG. 2, that is routed to these reading devices, via path 80. The digital scanner 30 converts the information on identification card 78 to machine understandable codes via a conventional optical character recognition technique and routes such converted information to the CPU 12 via the signal path 82. The magnetic reader 32 and the bar code scanner 34 each read the information present on the identification card 78 and supply respective output signals that are routed to decoder 36, via signal path 84 which, in turn, supplies machine readable signals to the CPU 12 via signal path 86. The signal paths 82 and 86 may be provided by wireless devices, such as, the wireless transmitter 50 and wireless receiver 62 both being conventional and both to be further described hereinafter. The usage of wireless devices may be advantageous if the digital scanner 30, magnetic reader 32 and bar code scanner 34 are remotely located relative to the CPU 12.

A clock source 38 supplies the clock signal, via signal path 88, to the CPU 12 that, in response to an appropriate computer program routine, establishes the time and date in which the information present on signal path 82, 84, 86 or 88 is read into and/or stored on the storage medium 20, 22 or 24. The CPU 12 under the direction of its computer programs, to be more fully described with reference to FIGS. 3 and 4, routes the information of the identification card 78, preferably encrypted as to be described hereinafter, via signal path 90 to the decrypter routine 40. The decrypter routine 40 decrypts the information and routes its non-encrypted information, via signal path 92, to a parser routine 42 which parses the information into jurisdictional segments, to be further described with reference to FIGS. 3 and 4, each having predetermined values. The parsed information is directed back to the CPU 12 via signal path 94. The CPU 12, performs a series of operations, under the direction of its computer programs, and provides, among other things, at least a verification signal, as well as human recognizable information that is placed on signal path 96 and routed to a first CRT display 44 via signal path 98 and to a second CRT display 56 via signal path 100.

The human recognizable information on signal path 98 also preferably contains a digital signal representation that is routed to the digital-to-analog (D/A) converter 46, which converts the digital representation into an analog signal representative of an audio signal. The digital signal representation also contains at least three bits each representative of verification signal conditions, such as YES, NO, and UNKNOWN to be used to respectfully flash GREEN, RED

US 6,463,416 B1

5

and AMBER LEDs of the LED array 58 to be further described with reference to FIG. 4(C). The digital-to-analog converter 46 is preferably excited by a D.C. voltage supply 48 which is also routed, via signal path 102, to a wiring hub 52 that also accepts the audio signal and the three bits (YES, NO and UNKNOWN) developed by the D/A converter 46. The wiring hub 52 is of a conventional type that arranges the received power and signal sources into appropriate cables, such as cable 104, that routes the representative audio signal from the D/A converter 46 to the speaker 60 and the three digital bits (YES, NO and UNKNOWN) as well as the excitation signal of the D.C. voltage supply 48 to the light emitting diode array 58. The wiring hub 52 may also include a switch that controls the on-off state of the excitation signal of the D.C. power supply 48 applied to one of the light emitting diodes 58 (and also to the CRT display 56 and speaker 60) so that the on-off power state of all elements 56, 58 and 60 may be remotely controlled from the wiring hub 52.

The speaker 60 may be a piezoelectric device that when activated by the audio signal developed by D/A converter 46 generates a buzzing sound that alerts an individual at the user's console 54 that the information (to be further described with reference to FIGS. 3 and 4) being displayed on either or both of the CRT displays 44 and 56 is not authentic. The CRT displays 44 and 56 are preferably of the type that is capable of handling text and graphics of the Super Video Graphics Array (SVGA) and/or National Television Standards Committee (NTSC).

The audio signal and the three bits (YES, NO and UNKNOWN) of the D/A converter 46 previously discussed and a signal representative that power is available from the D.C. voltage supply 48 may also be applied to the speaker 60 and light emitting diode array 58, by way of the wireless transmitter 50 cooperating with the wireless receiver 62 and interconnected thereto by signal path 106, with the output of the wireless receiver 62 being routed, via signal path 108, to speaker 60 and the light emitting diode array 58. The wireless transmitter 50, wireless receiver 62 and signal paths 106 and 108 are shown in phantom to indicate the alternate embodiment formed by the conventional wireless devices 50 and 62.

The speaker 60, and the CRT display 56 are both part of a user's console 54 and allow a user, such as a retailer to visually verify the authenticity of the information present on the identification card 78, such as a driver license, embodying human recognizable information and machine recognizable information generally illustrated in FIG. 2 which is comprised of FIGS. 2(A) and 2(B) that respectively show the front face 78A and the rear face 78B, each embodying information that is given in Table 2.

TABLE 2

{PRIVATE } REFERENCE NO.	INFORMATION
112	JURISDICTION (U.S. (STATE) OR CANADA (PROVINCE))
114	GRAPHIC OR LOGO OF JURISDICTION
116	DOCUMENT TYPE
118	NAME AND ADDRESS OF INDIVIDUAL OF THE DOCUMENT
120	PARTICULARS OF THE INDIVIDUAL OF THE DOCUMENT
122	SIGNATURE OF INDIVIDUAL OF THE DOCUMENT

6

TABLE 2-continued

{PRIVATE } REFERENCE NO.	INFORMATION
124	PHOTOGRAPH OF INDIVIDUAL OF THE DOCUMENT
126	IDENTIFICATION NUMBER OF DOCUMENT
128	DATE OF BIRTH (DOB)
130	US128 BAR-CODE
132	MAGNETIC STRIP
134	ANSI-20.1; 1993 CHARACTER SET OR 2D BAR CODE PDF-417
136	JURISDICTIONAL TEXT

The information given in Table 2 is read into the CPU 12 via signal paths 86 and the machine readable information 130, 132 and 134 on face 78B is preferably encrypted in a format preferably specified by ANSI-20.1; 1993 character set. The information 134 may also be encrypted in a format in accordance to a 2D bar code known as PDF-417 defined by the Symbol Technology Corporation of New York. The information 132 is also preferably decrypted and readable by the ANSI-20.1; 1993 Character Set and more fully described in "Recommendation for use of Magnetic Stripe on Drivers License" which is part of the NAFTA standard created and enforced by AAMVA which has been in existence in the United States and Canada since 1992 and is herein incorporated by reference.

In general, the operating programs residing in the CPU 12 authenticate the information embodied in the document, such as a driver license 78, having the particulars given in Table 2 each located at a predetermined region of the driver license 78 and corresponding to those of an individual and to those of a state or province in the United States or Canada, respectively, in which the individual legally resides but which are generally referred to herein as a jurisdiction. The particulars of the individual include height, weight, date of birth, sex and organ donor consent, whereas the particulars of the jurisdiction may include the state or province emblem or voting information. Further, the driver license 78 also includes graphics defining a background and/or a logo of the driver license 78. The operating program residing in the CPU 12 that authenticates these particulars and are comprised of a plurality of program segments represented by an overall sequence 140 illustrated in FIG. 3 and tabulated in Table 3.

TABLE 3

{PRIVATE } REFERENCE NO.	PROGRAM SEGMENT
142	START EVENT
144	DATA INPUT
146	DECODE DATA INPUT
148	SUBROUTINE FOR HANDLING OF LICENSE FORMAT
150	LICENSE FORMAT
152	DECRYPT DECODED INFORMATION
154	LICENSE FORMAT DETECT
156	DISPLAY ERROR MESSAGE
158	SAVE ERROR INFORMATION WITH TIME AND DATE
160	SUBROUTINE FOR HANDLING OF JURISDICTION FORMAT
162	JURISDICTION FORMATS
164	PARSE DECRYPTED INFORMATION
166	JURISDICTION FORMAT DETECT

US 6,463,416 B1

7

TABLE 3-continued

{PRIVATE } REFERENCE NO.	PROGRAM SEGMENT
168	SUBROUTINE FOR HANDLING OF LEGAL AGES
170	JURISDICTION LEGAL AGE
172	DETERMINE LEGAL AGES
174	OF LEGAL AGE
178	SUBROUTINE FOR HANDLING OF LICENSE BACKGROUND
180	LICENSE BACKGROUNDS
182	GENERATE LICENSE GRAPHICS
184	DISPLAY DATA
186	SAVE TRANSACTION WITH TIME AND DATE

The overall sequence 140 of FIG. 3 comprises the plurality of elements and has four (4) major subroutines 148, 160, 168 and 178 to be further described hereinafter respectively with reference to FIGS. 4(A), 4(B), 4(C) and 4(D). As used herein with reference to FIGS. 3 and 4, the program segments, sometimes referred to herein as processing segments, are shown as being interconnected by signal path and control is passed from one program segment to another when the output information of one program segment is placed on the signal path connected to the other program segment.

As seen in FIG. 3, and with simultaneous reference to FIG. 1, the overall program 140 is started by event 142 which initiates the reading of input data via signal path 82 or 86 of FIG. 1. With again reference to FIGS. 1, 2 and 3, the information embodied in driver license card 78 is read into CPU 12 via the digital scanner 30, magnetic reader 32 or bar code scanner 34 and represents the program segment 144 (input data) of FIG. 3. The operating program of CPU 12 routes the input data to program segment 146 via signal path 190 which, in turn, decodes the input data 144 and supplies the decoded information on signal path 192 to program segment 152.

The program segment 152 is part of subroutine 148, to be further described, that receives license format information from license format 150 and decrypts the information therein and provides such as the output of subroutine 148.

The output of subroutine 148 is applied to signal path 194 to program segment 154 which, like program segments 166 and 174, is a decisional segment which detects if the license format of the driver license 78 is correct, and if the format of the driver license 78 is correct, supplies the license format information to the processing segment 164 via signal path 196, but if the driver license 78 format is invalid, supplies the invalid license format on signal path 198 so that it is displayed on both CRT displays 44 and 56 shown in FIG. 1 as a display error message 156. The activation of the CRT displays 44 and 56 for the display error message 156, as well as other error displays and messages, is controlled by the CPU 12 servicing the input/output ports connected to the CRT displays 44 and 56. The displayed error message 156 is placed on signal path 200 which is routed to program segment 158 so that the error message is saved along with its time and date and the program segment 158 returns control to the start event 142 via signal path 202.

The program segment 164 is part of subroutine 160, to be further described, and receives jurisdiction formats information that is decrypted from program segment 162 which is also part of subroutine 160. The program segment 164 parses the decrypted information into jurisdictional seg-

8

ments having predetermined values, to be described with reference to FIG. 4(B). The program segment 164 supplies the decrypted information via signal path 204 to jurisdiction format detect program segment 166 which, in turn, detects if the jurisdictional format information 162 is correct, and if the information is correct, then the correct information is routed to program segment 172 via signal path 206, but if the information is incorrect then, the incorrect information is routed, via signal path 208, to the display error message program segment 156 which displays such an error on the CRT displays 44 and 56 of FIG. 1 and supplies that display error message to signal path 200 previously described.

The processing segment 172 is part of subroutine 168, to be further described, and receives jurisdictional legal ages information from program segment 170 which is also part of subroutine 168. Program segment 172 determines if the legal age requirements of the jurisdiction are met by the date of birth information of the driver license 78 and then sends its determined information, via signal path 210 to decisional segment 174. If the decisional segment 174 detects that the legal age has been satisfied, it routes this information onto program segment 182 via signal path 212, but if the legal age information is incorrect, then an error notification (display error message) is routed to program segment 156 via signal path 204. Program segment 156 responds in a manner as previously described.

The processing segment 182 is part of subroutine 178, to be further described, and receives the license background of the particular jurisdiction from program segment 180, also part of subroutine 178. The program segment 182 generates license graphics and places such on signal path 216 applied to program segment 184 which, in turn, is transferred as output displays to the CRT displays 44 and 56 of FIG. 1. Program segment 184 applies its output on signal path 218 which in turn, is routed to program segment 186 which saves the transaction along with its time and date. The processing segment 186 provides notification, via signal path 219 to the next start event 142 which, in turn, causes the sequence of the next overall segment 140 having four subroutines, the first of which may be further described with reference to FIG. 4(A) which is comprised of a plurality of program segment tabulated in Table 4.

TABLE 4

{PRIVATE } REFERENCE NO.	PROGRAM SEGMENT
220	GET DECODED DATA
222	GET UNENCRYPTED JURISDICTION FROM DECODED DATA
224	LOAD STORED JURISDICTION "KEYS"
226	DECRYPT DATA
228	PARSE DATA INTO 3-5 TRACKS DEPENDING ON JURISDICTION
230	READING TRACK DATA LOOP
232	GET NEXT TRACK OF DATA
234	TRACK BLANK
236	STORE VALUES FOR TRACK
238	STORE BLANK VALUES FOR TRACK
240	ALL TRACKS BLANK
242	ANY TRACKS BLANK
244	DISPLAY "BLANK CARD" MESSAGE
246	DISPLAY "INVALID LICENSE" MESSAGE
248	STORE ERROR INFORMATION

The subroutine 148 of FIG. 4(A) is initiating with start procedure event 192 and is terminated with the end procedure event 194, wherein events 192 and 194 correspond to the signal paths shown in FIG. 3. It should be noted that



US 6,463,416 B1

9

program segments 150 and 152 shown in FIG. 3 as making up subroutine 148 are not shown in FIG. 4(A) because the programming functions performed by segments 150 and 152 are integrated and blended into the plurality of elements of FIG. 4(A). This same rationale is applicable to the program segments 162-164, 170-172 and 180-182 of FIG. 3 that have been blended into the program segments of FIGS. 4(B), 4(C), and 4(D) respectively to be further described hereinafter.

With reference to FIG. 4(A), the output of start procedure event 192 is applied to signal path 250 which is routed to program segment 220. The program segment 220 retrieves the decoded data shown in FIG. 3 as program segment 146 (decode data input) and provides such information on signal path 252 which is applied to program segment 222.

Program segment 222 retrieves the unencrypted jurisdiction data specified in the decoded data of program segment 220 and routes such information on signal path 254 which is applied to program segment 224. Program segment 224 loads the jurisdiction "keys" which identifies a record for the jurisdictional segment. More particularly, the "keys" identify the tracks on the storage mediums 20, 22, 24 where jurisdiction segments are stored so that the license format of the jurisdiction segment under consideration may serve as the predetermined values of subroutine 148 to which the format of the data of the driver license 78 read into the CPU 12 may be compared and authenticated as being correct. The comparison and authentication of the predetermined values of the jurisdictional segments is also accomplished for subroutines 160, 168 and 178 to be described.

The information loaded by program segment 224 is applied to signal path 256 that is routed to program segment 226 which decrypts the data it receives from program segment 224 and routes such decrypted data on signal path 258 which, in turn, is applied to program segment 228.

The program segment 228 parses the data into 3-5 tracks, dependent on the jurisdictional segment specified by the decoded data of program segment 220. The parsed data of program segment 228 is applied to signal path 260 which, in turn, is applied to program segment 232 which is part of the reading track data loop 230 which is repetitively repeated 3-5 times dependent upon the jurisdictional segment specified by the data of program segment 220. More particularly, for example, if one jurisdiction (representative of a state in the United States or of a province in Canada) requires three (3) tracks of storage, loop 230 is repetitively repeated three (3) times.

The first program segment 232 of loop 230 retrieves the next or first track of data of the information present on signal path 260 and routes such information to decisional segment 234 which, if the track information is blank, provides that determination on signal path 264 and, conversely, if the track is not blank provides that determination on signal path 266 which is applied to program segment 236. Program segment 236 stores the values for the retrieved track of data and after it is stored applies an appropriate signal on signal path 268 to pass control to program segment 238 that also has signal path 264 from program segment 234 applied thereto.

Program segment 238 stores the blank value for the retrieved track. If all blank values have not been stored then program segment 238 returns control to program segment 232 by way of signal path 270 but, if all blank values have been stored then program segment 238 passes control to program segment 240 via signal path 272.

Program segment 240 determines if all the tracks assigned for the particular jurisdiction under consideration are blank and if so provides knowledge thereof on signal path 274.

10

Conversely, if all tracks are not blank, the program segment 240 passes control, via signal path 276, to program segment 242.

Program segment 242 determines if any tracks are blank and if the answer is yes then provides a notification thereof on signal path 280 however, if the answer to the question "any tracks blank" is no, (which signifies a correct condition) then program segment 242 passes control to the end procedure event 194 via signal path 278 which, in turn, returns to the overall step-by-step procedure 140 shown in FIG. 3. If signal path 274 or 280 is activated, then program segment 244 or 246, respectively, is activated and an alarm message is displayed on the CRT displays 44 and 56 of FIG. 1 and then control is passed to program segment 248. Program segment 248 stores the alarm message of program segment 244 or 246 and then passes control to signal path 284 which, in turn, provides notification to the end procedure event 194 which allows the program to return to the overall procedure 140 of FIG. 3. The program segment 140 of FIG. 3 sequences until it reaches signal path 196 which initiates the subroutine 160 of FIG. 4(B) that is comprised of a plurality of program segments that are tabulated in Table 5.

TABLE 5

{PRIVATE } REFERENCE NO. PROGRAM SEGMENT	
286	GET DECRYPTED DATA
288	LOAD STORED JURISDICTION FORMAT
290	PROGRAM LOOP FOR GATHERING TRACK DATA FOR JURISDICTION FORMAT
292	GET NEXT TRACK OF DATA
294	PARSE TRACK DATA ACCORDING TO JURISDICTION FORMAT
296	DATE MATCHED JURISDICTION FORMAT
298	DISPLAY "FRAUDULENT CARD" MESSAGE
300	STORE INDIVIDUAL VALUES INTO DRIVER LICENSE FIELDS
302	STORE ERROR INFORMATION WITH TIME & DATE
304	LOAD STORED JURISDICTION DATA
306	FRAUD CHECKSUM
308	PROGRAM LOOP FOR PERFORMING PARITY CHECKSUM
310	PERFORM PARITY CHECKSUM ON TRACK DATA
312	DATA MATCHED JURISDICTION FORMAT
314	DISPLAY "TAMPERED CARD" MESSAGE
	STORE ERROR INFORMATION WITH TIME & DATE

As seen in FIG. 4(B) the subroutine 160 is initiated by start procedure event 196 and terminated by end procedure event 204 each of which events corresponds to the signal path having the same reference number shown in FIG. 3. The notification of the start procedure event 196 is applied on signal path 316 which is routed to program segment 286 which, in turn, retrieves the decrypted data originally loaded into the CPU via program segment 144 of FIG. 3. Program segment 286 activates signal path 318 that is routed to program segment 288 which loads the stored jurisdictional format defining the format related to the jurisdiction of the individual specified in the driver license 78 loaded into the CPU 12. After such loading, program segment 288 passes control over to program loop 290 via signal path 320.

The first segment of loop 290 is program segment 292 which retrieves the first or next track of data defined by program segment 288 and passes control over to program

US 6,463,416 B1

11

segment 294 via signal path 322. Program segment 294 parses the retrieved track data according to the particular jurisdictional format under consideration and passes control over to program 296 via signal path 324.

Program segment 296 is a decisional segment that matches the data from program segment 292 to the jurisdictional format under consideration, and if a proper match exists passes control over to program segment 300 via signal path 326, but if a match does not occur, passes control over to program segment 298 via signal path 328.

Program segment 298 causes the display of the message "fraudulent card" on the CRT displays 44 and 56 of FIG. 1 and then passes control over to program segment 302 via signal path 330. Program segment 302 stores the error information along with its time and date and passes control over to program segment 304 via signal path 332.

Program segment 300 receive control from signal paths 326 and 332 and stores the individual values of the driver license data read into the CPU 12 into the driver license fields in the CPU 12.

Program segment 300 returns control, via signal path 334, to program segment 292 which, as previously mentioned, is the first step of loop 290. Loop 290 has a repetitive cycle between 3 to 5 times dependent on the jurisdictional segment and for each repetitive cycle program segment 300 passes control over to program segment 292 via signal path 334, and when loop 290 is complete, program segment 300 passes control over to program segment 304 via signal path 332. The interaction of loop 290 serves as a fraudulent check which in actuality detects any counterfeit documents.

Program segment 304 loads the stored jurisdiction checksum and and passes control over to program loop 306 having a first program segment, that is, program segment 308. The checksum determines if the data has been tampered with or altered after having been officially issued.

Program segment 308 performs the parity checksum on the track data received from program segment 304 and then passes control onto program segment 310 via signal path 338.

Program segment 310 performs a data match of the jurisdictional format and if the data is not correct passes control over to program segment 312 via signal path 340. Program 20 segment 312 causes the CPU 12 to activate the CRT displays 44 and 56 of FIG. 1 and display the error message "tampered card" and then passes control over to program segment 314 via signal path 342. Program segment 314 stores the error information along with its time and date and passes control to end procedure event 204 via signal path 344. End procedure event 204 also receives control from program segment 310 via signal path 346 if the data match jurisdictional format performed by program segment 310 is correct. End procedure event 204 returns control back to the overall program segment 140 of FIG. 3 which sequences to subroutine 168 of FIG. 4(C) which is comprised of a plurality of program segments which are tabulated in Table 6.

TABLE 6

{PRIVATE }REFERENCE NO.	PROGRAM SEGMENT
348	LOAD STORED CATEGORY AGENTS
350	GET INDIVIDUAL'S AGE
352	PROGRAM LOOP FOR GATHERING CATEGORY AGE

12

TABLE 6-continued

{PRIVATE }REFERENCE NO.	PROGRAM SEGMENT
354	GET CATEGORY AGE
356	AGE = > CATEGORY AGE
358	SET CATEGORY RESULTS TO FALSE
360	SET CATEGORY RESULTS TO TRUE
362	GET PRIMARY AGE CATEGORY
364	AGE = > PRIMARY CATEGORY AGE
366	FLASH AMBER LED
368	FLASH RED LED's
370	FLASH GREEN LED's

As seen in FIG. 4(C), the subroutine 168 is initiated by the start procedure event 206 and is terminated by the end procedure event 212, with the events corresponding to signal paths 206 and applied upon single path 374 which notifies program segment 348. Program particular jurisdictional segment under consideration, and the passes control over to program segment 350 via signal path 376. The category ages may include the legal age for drinking and voting.

Program segment 350 retrieves the individual's age from the initial data read into the CPU 12 by program segment 144 of FIG. 3. The program segment 350 passes, via signal path 378, control over to the program loop 352 which is repetitively performed 5 times and has a first program segment 354.

Program segment 354 retrieves or gets the next or first category age of program segment 350 and passes, via signal path 380, control over to program segment 356. Program segment 356 determines if the age of the individual is within the category of ages for the jurisdictional segment, and if the answer is yes, then passes control over to program segment 360 via signal path 382 and, conversely, if the category age is not correct passes control over to program segment 358 via signal path 384. Program segment 358 sets the category results false, and then passes, via signal path 386, control back to program segment 354 which, as previously discussed, is the first program segment of the loop 352.

Once the loop is iterated 5-times, then either program segment 358 or 356 passes control over to program segment 362, via signal path 388.

Program segment 362 retrieves the primary age category, that is, for example, the legal age of drinking in the particular jurisdiction, and then passes control to program segment 364 via signal path 390.

Program segment 364 determines the age of the individual designated by the contents of the driver license 78 read into the CPU 12, and, more particularly, determines if the age is below the required legal age. Program segment 364 in its determination sets one of the three (3) digital bits previously discussed with regard to the D/A converter 46 that is past onto the LED array 58, both previously described with reference to FIG. 1. If the age of the individual does not at least equal that required by the jurisdiction for the selected category, such as drinking, program segment 364 passes control over to the program segment 368, via signal path 392A, which causes the CPU 12 to have a RED indicator of the LED array 58 flashed. If program segment 364 is unable to determine the age category, it passes, via signal path 392B, control over to program segment 366 which, in turn, causes the CPU 12 to have the amber LED of the LED array 58 flashed. If program segment 364 determines the primary age to be correct, program segment 364 passes control over to program segment 370, via signal path 392C. Program

US 6,463,416 B1

13

segment 370 causes the CPU 12 to have the green LED of the array 58 flashed. Once the LED flashing is completed, program segment 370 passes, via signal path 394, control over to the end procedure event 212 which, in turn, allows the subroutine 168 to be returned to the overall program segment 140 of FIG. 3 which, in turn, allows the program segment 140 to sequence to subroutine 178 which may be further described with reference to FIG. 4(B) comprised of a plurality of program segments that are tabulated in table 7.

TABLE 7

{PRIVATE }REFERENCE NO. PROGRAM SEGMENT	
396	GET JURISDICTION ID & CODE
398	LOAD STORED LICENSE BACKGROUND
400	DISPLAY LICENSE BACKGROUND
402	UNDER LEGAL AGE
404	LOAD STORED UNDER AGE GRAPHICS
406	DISPLAY UNDER AGE GRAPHICS
408	DETERMINE AGE LOOP
410	PROGRAM LOOP FOR DETERMINE AGE CATEGORY
412	GET NEXT CATEGORY AGE
414	AGE = > CATEGORY AGE
416	DISPLAY "NO" SYMBOL
418	DISPLAY "YES" SYMBOL
420	GET DRIVER CLASS
422	LOAD STORED CLASS GRAPHICS
424	DISPLAY CLASS GRAPHICS

As seen in FIG. 4(D), the subroutine 178 is initiated with the start procedure event 212 and terminated with the end procedure event 216 which correspond to the signal paths 212 and 216 of FIG. 3. The occurrence of the start procedure event 212 is passed to the program segment 396 by the way of signal path 426.

Program segment 396 retrieves the jurisdiction identification (ID) and the code of the driver license 78, which is a code indicating the AAMVA assigned Jurisdiction Number and a Code which jurisdiction at the time of encrypting. Program segment 396, after its completion, passes control over to program segment 398 via signal path 428.

Program segment 398 loads the stored license background that was read into CPU 12 by the program segment 144 of FIG. 3. Program segment 398 passes control over to program segment 400 by way of signal path 430.

Program segment 400 displays the license background on the CRT displays 44 and 56 of FIG. 1 and passes control over to program segment 402 via signal path 432.

Program segment 402 determines if the age on the driver license is, for example, under 21 (Legal Age) and if the answer is yes, passes control over to program segment 404 via signal path 434, but if the answer is no, passes control to program segment 408 via signal path 436.

Program segment 404 loads the stored under age graphics and passes control over to program segment 406 via signal path 438 which causes the CPU 12 to have the CRT displays 44 and 56 of FIG. 1 display the under age graphics. The under age graphics may be selected to attract the attention of the user of the authentication system 10 of the present invention. After such display the program segment 406 passes control over to program segment 408 via signal path 440.

Program segment 408 is an age determining segment loop which is accomplished by a program loop 410 interlinked to program segment 408 via signal paths 442 and 444.

The first program segment of program loop 410 is program segment 412 which retrieves the next age category

14

which, for example, may be the age for smoking and passes control over to program segment 414 via signal path 446.

Program segment 414 determines if the age of the individual of the driver license 78 read into the CPU 12 is equal to or greater than the category age. The categories include alcohol, tobacco, lottery, gambling and custom guidelines used for casino or for entrance into an entertainment facility. If the answer of program segment 414 is yes, program segment 414 passes control over to program segment 418 via signal path 448, but if the answer is no, program segment 414 passes control over to program segment 416 via signal path 450.

Program segment 416 causes the CPU to provide the "no" symbol on the CRT displays 44 and 56 of FIG. 1, whereas program segment 418 causes the CPU 12 to cause the display of the "yes" symbol on the same CRT displays 44 and 56. The "yes" and "no" symbols may be selected to attract the attention of the user of the authentication system 10 of the present invention. The program loop 410 is typically and repetitively repeated five (5) times and upon such completion passes control back to the program segment 408 via signal path 444.

Program segment 408 after its completion passes control over to program segment 420 via signal path 454.

Program segment 420 retrieves the driver class designation and passes control over to program segment 422 via signal path 456. Program segment 422 loads the stored driver class graphics and passes control over to program segment 424 via signal path 458.

Program segment 424 causes the CPU 12 to display the class graphics on the CRT displays 44 and 56 of FIG. 1 and upon its completion passes, via signal path 460 control to end procedure event 216 which is also shown as signal path 216 of FIG. 3.

As seen in FIG. 3, the signal path 216 notifies the program segment 184 of the generation of license graphics which, in turn, passes control over to program segment 186 via signal path 218 which, in turn, passes control back to the start event 142, via signal path 220 so that the overall program 140 of FIG. 3 may be repeated, if necessary.

It should now be appreciated that the practice of the present invention provides for an authentication system 10 to authenticate driver licenses that are coded with machine readable information in accordance with AAMVA standards, as well as coded with human recognizable information.

It should be further appreciated that the present invention, not only verifies the contents of driver licenses but also allows the information contained in the CPU 12 to be transferred to a remote or local jurisdiction, via modem 26, to remote computer 28 so that the information may be identified for criminal prosecution purposes or, conversely, for humanitarian purposes, such as, for identifying preordained organ donors. The identification for criminal or humanitarian purposes may be accomplished in a manner similar to that hereinbefore described with reference to FIGS. 1-4.

Furthermore, it should be appreciated that the present invention provides the means for not only rapidly authenticating a document, such as a driver license, but also allowing the driver license to serve as a convenient means for rapidly verifying that age requirements are satisfied in any purchase at the point-of-transaction or in allowing ingress into establishments having their own age requirements.

Further still, it should be appreciated that the practice of the present invention utilizes a personal computer, such as CPU 12, commonly found in many places of businesses used



US 6,463,416 B1

15

for inventory purposes but also having a need to authentic-  
ating the contents of a driver license, such as authenticating  
identification for credit card and check writing at the point-  
of-sale. Further uses could be to authenticate driver licenses  
in police cars, ports of entry such as domestic and internal  
airports, sea ports, rail stations and border check-points.  
Attached to existing locking mechanisms, could be inte-  
grated into lottery, tobacco and alcohol vending machines  
and to points of entry to buildings and other sensitive areas.  
Verifying identity is also important to other areas such as  
child day care centers and Post Offices to verify parcel  
pick-up and drop-off.

What is claimed:

1. A programmable apparatus for authenticating a docu-  
ment which embodies identification information for an iden-  
tified entity comprising both human recognizable informa-  
tion and machine recognizable coded information, said  
apparatus comprising:

means for reading the information of said document into  
said programmable apparatus;

means for determining whether said document includes a  
license format corresponding to a reference license  
format based on a comparison between said read infor-  
mation and said reference license format;

means for parsing said read information into jurisdictional  
segments if said license format matches said reference  
license format, wherein reference jurisdictional seg-  
ments as included in said reference license format each  
have predetermined values;

processing means directing the operation of said program-  
mable apparatus for comparing said read information to  
determine whether said jurisdictional segments match  
said predetermined values;

said processing means further directing the operation of  
said programmable apparatus for determining whether  
a selected identification parameter for said identified  
entity corresponds to a preselected criterion and gen-  
erating at least a verification signal if said selected  
identification parameter satisfies said preselected crite-  
rion; and

means for indicating a verification signal.

2. The programmable apparatus of claim 1 wherein said  
means for indicating a verification signal is manifested as a  
display means selected from the group consisting of:

means for displaying read information from a license  
format,

means for displaying alarm messages,

means for displaying error messages, and

means for displaying a "yes" or "no" message.

3. The programmable apparatus of claim 1, wherein said  
means for indicating a verification signal is capable of  
providing human recognizable information in text and  
graphics, said text and graphics being capable of utilizing  
programs including the Super Video Graphics Array, and  
National Television Standards.

4. A method for authentication of an identification criteria  
in an identification document, said identification document  
containing a set of information segments related to an entity  
subject to identification, said information segments being  
organized according to one of a plurality of known formats,  
said method comprising the steps of:

extracting at least a portion of said set of information  
segments included in said identification document, said  
extracted portion including a manifestation of said  
identification criteria;

16

retrieving reference data from a storage means in respect  
to said known organizational format and comparing  
said extracted information segments with said retrieved  
format data to determine conformance of said extracted  
information segments with said known organizational  
format;

upon making said conformance determination, selecting  
said information segment corresponding to said iden-  
tification criteria and comparing it to a predetermined  
acceptance criteria;

providing a signal indicative of whether said predeter-  
mined acceptance criteria is met by said identification  
criteria.

5. The authentication method of claim 4 wherein said  
identification document is associated with a particular issu-  
ing jurisdiction and further wherein identification docu-  
ments so associated with said particular issuing jurisdiction  
are uniformly based on a common one of said known  
organizational formats.

6. The authentication method of claim 2 wherein said step  
of comparing said extracted information segments with said  
removed format data includes the substeps of:

determining an identity of an issuing jurisdiction for said  
identification document; and

performing a lookup in a stored database to find said  
common one of said known organizational formats for  
the jurisdiction so identified.

7. The authentication method of claim 6 wherein a speci-  
fied plurality of required information segment records is  
defined for ones of said plurality of known organizational  
formats, and further wherein said step of comparing said  
extracted information segments with said retrieved format  
data includes the further substeps of:

comparing said required information segment records for  
said common one of said known organizational formats  
for the identified jurisdiction with said information  
segments extracted from said identification document;  
and

determining whether a correspondence exists between  
each of said required information segment records and  
one of said extracted information segments.

8. The authentication method of claim 7 wherein the  
substep of the comparing said required information segment  
records with said extracted information segments includes  
the further substep of:

parsing said extracted set of information segments into  
individual ones of said set.

9. The authentication method of claim 6 wherein ones of  
said plurality of known organizational formats define a  
particular ordering of data for information segment records  
included in said identification document, and further  
wherein said step of comparing said extracted information  
segments with said retrieved format data includes the further  
substeps of:

comparing a data ordering of ones of said extracted  
information segments with a data ordering for an  
associated information segment record as defined by  
said common one of said known organizational formats  
for said identified issuing jurisdiction; and

determining whether a correspondence exists between an  
information segment data ordering and a format-  
defined data ordering for an associated information  
segment record for each of said extracted information  
segments.

10. The authentication method of claim 9 wherein said  
substep of comparing a data ordering includes the further  
substep of:

US 6,463,416 B1

17

parsing said ones of said extracted information segments to provide a segmentation thereof corresponding to said format-defined data ordering.

11. The authentication method of claim 4 wherein said step of comparing said extracted information segments with said retrieved format data includes the further substep of:

performing an error check on ones of said extracted information segments relative to an expected value of said information segment, said expected value being determined in respect to said known organization format.

12. The authentication method of claim 11 wherein said error check includes an application of a checksum to a value of ones of said extracted information segments.

13. The authentication method of claim 4 wherein said identification criteria is a date of birth and said predetermined acceptance criteria is a date corresponding to a minimum age for said entity subject to identification.

14. The authentication method of claim 4 wherein said set of information segments are manifested in said identification document in a form selected from machine recognizable, human recognizable, or both.

15. The authentication method of claim 14 wherein said step of information segment extraction is implemented by operation of a magnetic reader or bar-code scanner when said set of information segments is in a machine recognizable form.

16. The authentication method of claim 14 wherein said step of information segment extraction is implemented by operation of a digital scanner when said set of information segments is in a human recognizable form.

17. The programmable apparatus of claim 1 wherein said reading means is a keyboard.

18. The programmable apparatus of claim 1 wherein said reading means is a digital scanner.

19. The programmable apparatus of claim 1 wherein said reading means is a magnetic reader.

20. The programmable apparatus of claim 1 wherein said reading means is a bar code scanner.

21. The programmable apparatus of claim 1 wherein said reading means is selected from the group consisting of a keyboard, a digital scanner, a magnetic reader and a bar code scanner.

18

22. The programmable apparatus of claim 1 wherein said reading means is any two devices selected from the group consisting of a keyboard, a digital scanner, a magnetic reader and a bar code scanner.

23. The programmable apparatus of claim 1 wherein said reading means is any three devices selected from the group consisting of a keyboard, a digital scanner, a magnetic reader and a bar code scanner.

24. A programmable apparatus for authenticating an identification document of an individual comprising:

a reader adapted read information from said identification document;

a processor under the control of software including:

a jurisdiction discriminator engine adapted to determine and authenticate a jurisdiction that originated said identification document using said information; and

a comparator adapted to compare segments of said information to a predetermined acceptance criteria and generate a result; and

a reporting device adapted to provide results of said comparator.

25. The programmable device of claim 24 wherein said jurisdiction discriminator includes a comparator for comparing said information to jurisdictional reference data.

26. The programmable device of claim 24 wherein said jurisdictional discriminator is adapted to compare said information to known jurisdictional formats for said information to determine an origin.

27. The programmable device of claim 24 wherein said reader is selected from the group consisting of a keyboard, a digital scanner, a magnetic reader and a bar code scanner.

28. The programmable device of claim 24 wherein said comparator is adapted to compare information relating to an age of said individual with a known age limit.

29. The programmable device of claim 28 wherein said age limit is selected from the group of activities having minimum ages consisting of purchasing alcohol, purchasing cigarettes and gambling.

\* \* \* \* \*