US005615277A

United States Patent [19]

Hoffman

[11] **Patent Number: 5,615,277**

[45] **Date of Patent: Mar. 25, 1997**

[54] **TOKENLESS SECURITY SYSTEM FOR AUTHORIZING ACCESS TO A SECURED COMPUTER SYSTEM**

[76] Inventor: **Ned Hoffman**, 2529A College Ave.,
Berkeley, Calif. 94704

[21] Appl. No.: **345,523**

[22] Filed: **Nov. 28, 1994**

[51] **Int. Cl.**^{6} **G06K 9/00**

[52] **U.S. Cl.** **382/115**; 902/3

[58] **Field of Search** 340/825.34, 825.33, 340/825.31; 382/115, 116, 117, 118, 119, 124, 128; 902/1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 22, 23, 24, 25, 26, 27, 31, 32, 33, 34, 35, 37; 235/375, 376, 379, 380, 381, 382, 382.5, 383, 384, 385, 386

[56] **References Cited**

U.S. PATENT DOCUMENTS

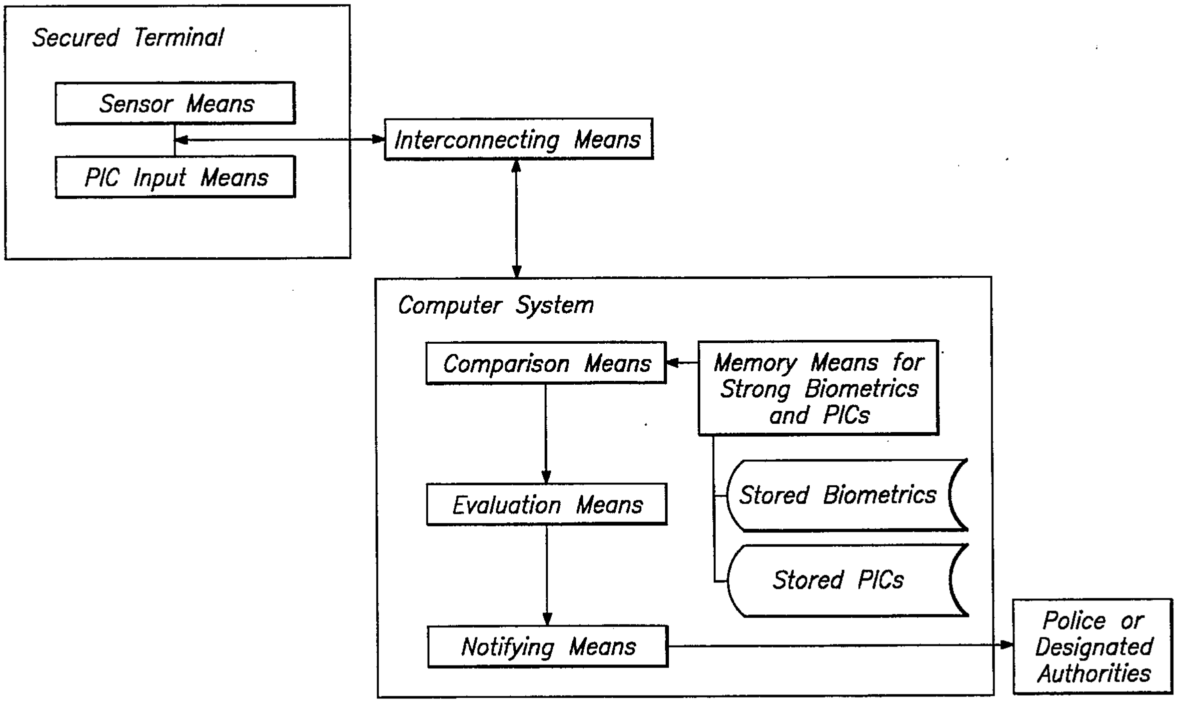
4,961,142	10/1990	Elliott et al.	364/408
5,036,461	7/1991	Elliott et al.	364/408
5,229,764	7/1993	Matchett et al.	340/825.34

Primary Examiner—Jose L. Couso
Assistant Examiner—Bijan Tadayon
Attorney, Agent, or Firm—Ali Kamarei

[57] **ABSTRACT**

A tokenless security system and method for preventing unauthorized access to one or more secured computer systems is shown. The security system and method are principally based on a correlative comparison of a unique biometric sample, such as a finger print or voice recording, gathered directly from the person of an unknown user with an authenticated unique biometric sample of the same type obtained from each authorized user. The security system and method may be integrated with and dedicated to a single computer system, or may be configured as a non-dedicated, stand-alone entity capable of and intended to perform security functions simultaneously for more than one computer system. Further, the stand alone configuration can be networked to act as a full or partial intermediary between a secured computer system and its authorized users, or may be interactive solely with and act as a consultant to the computer systems. The security system and method further contemplate the use of personal codes to confirm identifications determined from biometric comparisons, and the use of one or more variants in the personal identification code for alerting authorities in the event of coerced access.

113 Claims, 3 Drawing Sheets



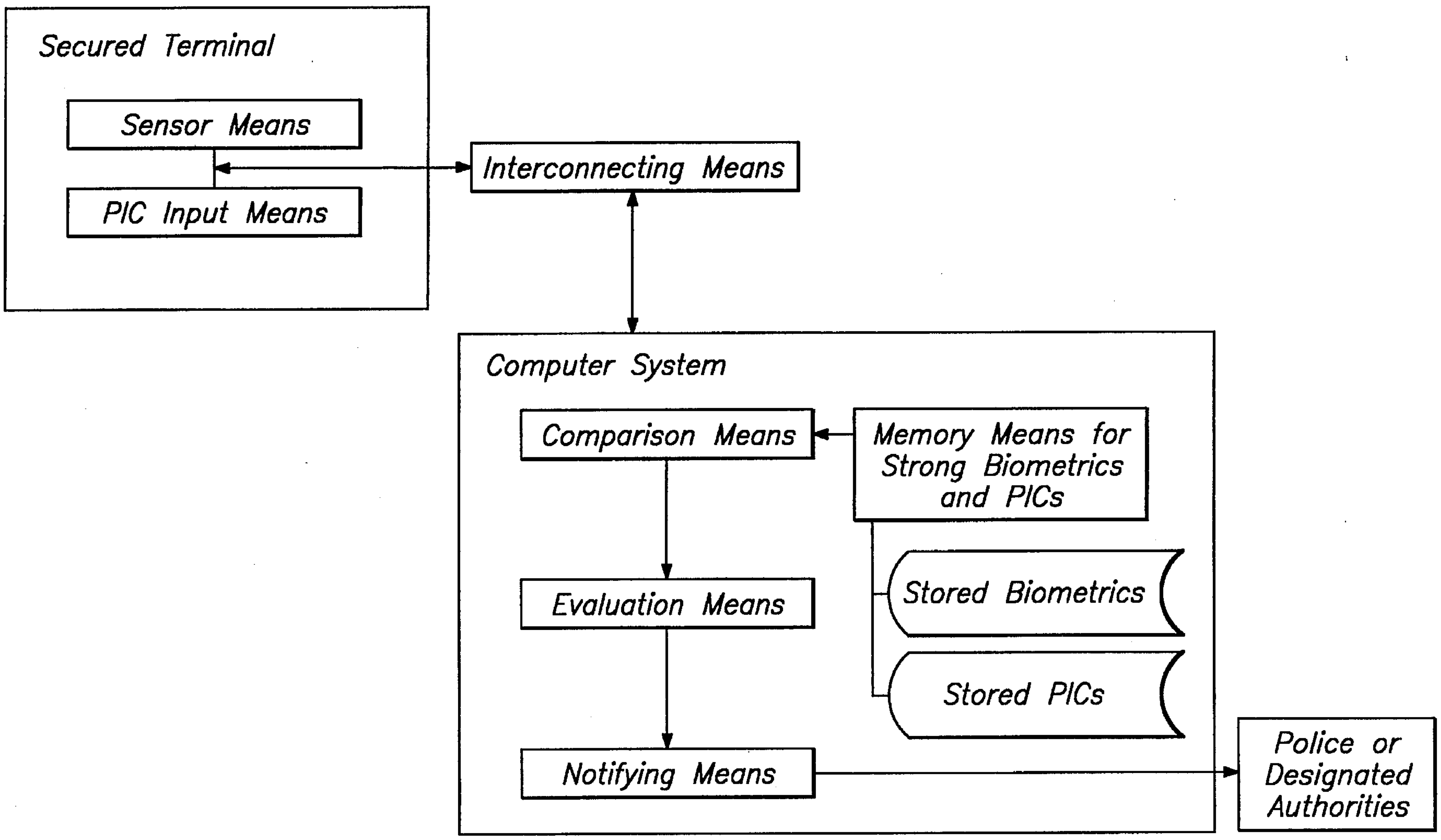

Secured Terminal
Sensor Means
PIC Input Means
Interconnecting Means
Computer System
Comparison Means
Memory Means for Strong Biometrics and PICs
Stored Biometrics
Stored PICs
Evaluation Means
Notifying Means
Police or Designated Authorities

FIG. 1

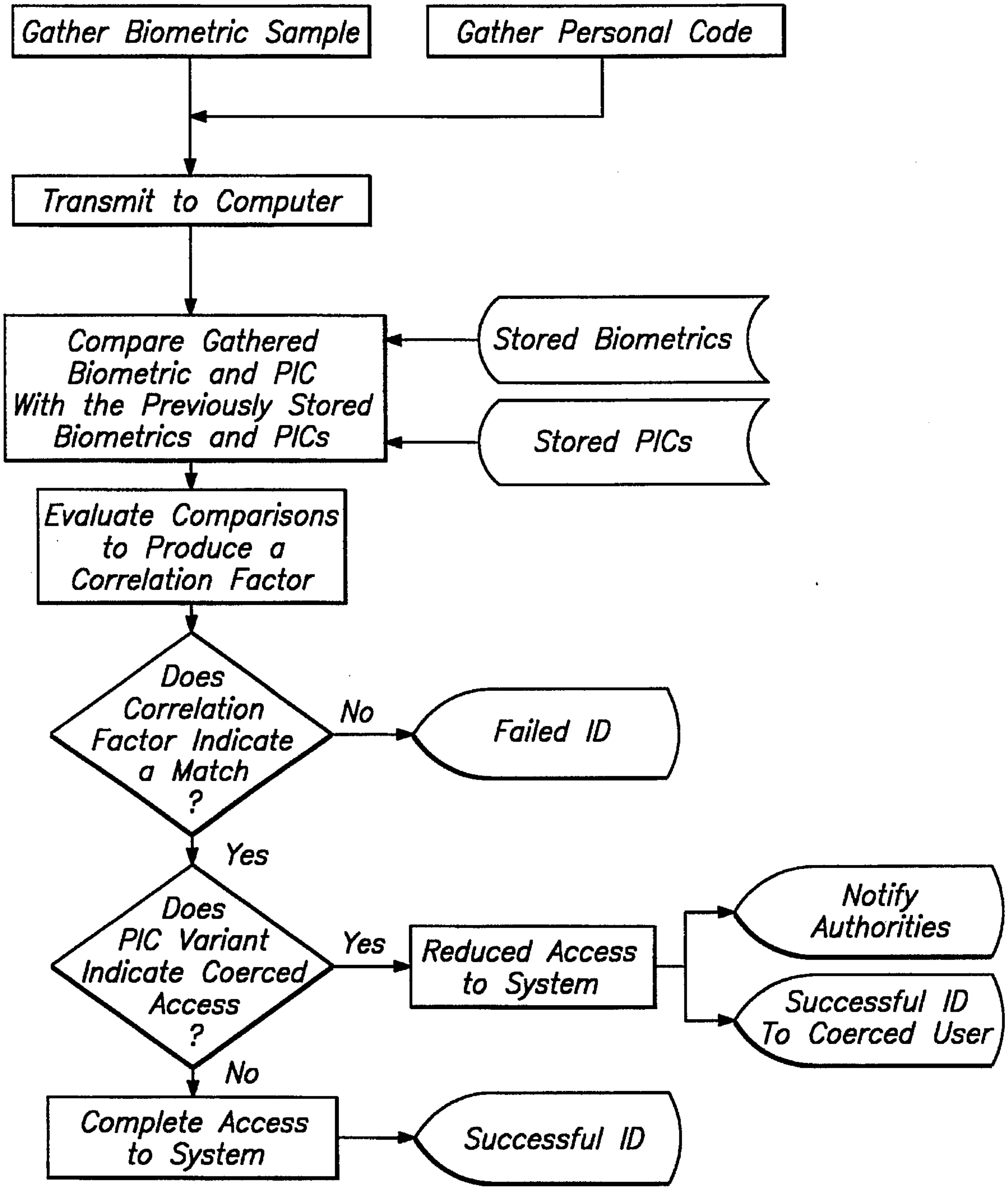

Gather Biometric Sample
Gather Personal Code
Transmit to Computer
Compare Gathered Biometric and PIC With the Previously Stored Biometrics and PICs
Stored Biometrics
Stored PICs
Evaluate Comparisons to Produce a Correlation Factor
Does Correlation Factor Indicate a Match ?
No
Failed ID
Yes
Does PIC Variant Indicate Coerced Access ?
Yes
Reduced Access to System
Notify Authorities
Successful ID To Coerced User
No
Complete Access to System
Successful ID

FIG. 2

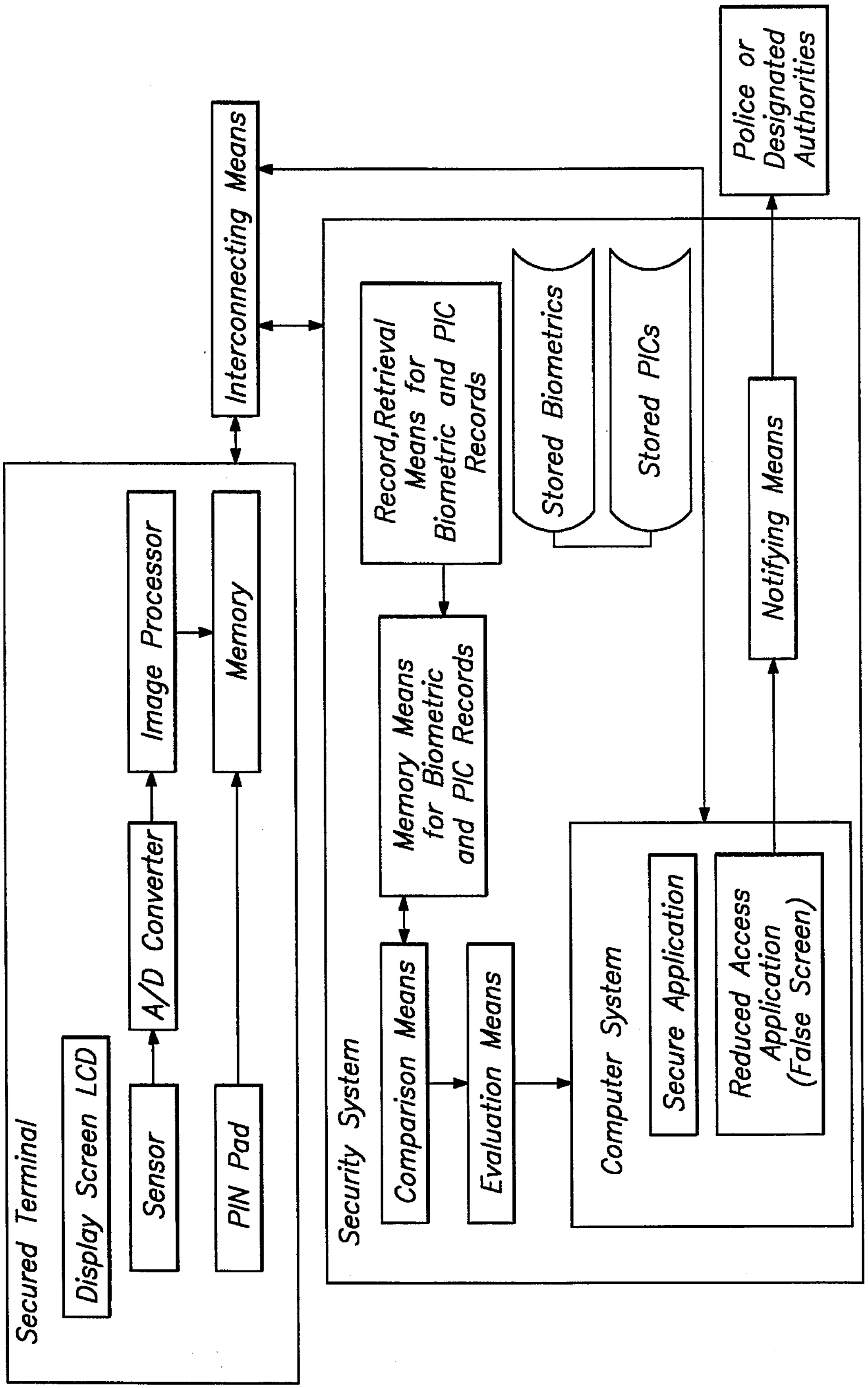

Secured Terminal
Display Screen LCD
Sensor
A/D Converter
Image Processor
PIN Pad
Memory
Interconnecting Means
Security System
Record,Retrieval Means for Biometric and PIC Records
Stored Biometrics
Stored PICs
Memory Means for Biometric and PIC Records
Comparison Means
Evaluation Means
Computer System
Secure Application
Reduced Access Application (False Screen)
Notifying Means
Police or Designated Authorities

FIG. 3

TOKENLESS SECURITY SYSTEM FOR AUTHORIZING ACCESS TO A SECURED COMPUTER SYSTEM

FIELD OF THE INVENTION

The invention relates generally to security systems designed to control access to restricted areas, and more specifically to security systems for controlling individual access to secured computer systems.

BACKGROUND OF THE INVENTION

The rapid, efficient and secure transaction of financial and other services is becoming critical to the competitiveness of individual businesses and national economies. In the past, financial transactions were necessarily slow and cumbersome, generally requiring an individual to verify his identity by meeting with a representative of the financial institution responsible for executing the transaction. Although inconvenient and somewhat inflexible, such systems were useful in reducing transaction fraud because they predicated verification of the individual's identity based on certain unique biometric data, such as one's signature, physical appearance, voice character, etc, in addition to the individual's personal knowledge of his financial account numbers and secret codes.

With the advent of computerized financial networks, the problem of transaction fraud has become keenly acute, facing not only private business, but local, state and federal governments as well. In order to cut costs and increase the flexibility of making financial transactions, many financial institutions have greatly reduced staff and office hours in favor of automated teller machines ("ATM"s), which provide the consumer with round the clock access to his various accounts and allow the consumer to make financial transactions without visiting a bank. More recently, retail establishments have taken advantage of the existence of such computerized banking services by installing apparatus capable of reading a consumer's ATM card and making a direct debit from the consumer's account at the point of purchase. Unfortunately, the use of ATMs and similar devices has greatly increased transaction fraud because in such systems verification of a user's identity is not predictated on unique biometric data. Rather, all that is required for verification is the presentation of a token, such as a credit card or ATM, and the entry of the personal identification number ("PIN") encoded in a magnetic strip on the token. It is estimated that billions of dollars are lost annually through transaction fraud. Ultimately, these costs are passed back to the consumer in the form of higher prices for goods and services, and in the form of higher taxes.

Today, a considerable proportion of financial transactions, stock trading, commodity trading, business purchases and billings are transacted electronically. In these systems, the necessary data for identifying and locating the user's accounts are magnetically recorded on a token that user must insert into the ATM or similar device to initiate access to his accounts. The token is further provided with a personal identification number ("PIN"), which ideally is known only to the user and the financial institution controlling the account. Although the combination of an account number and PIN will be unique to the user, the ability to possess and communicate such data will not be unique to the user. Rather, existing security systems of computer networks will recognize anyone capable of entering the appropriate account and PIN as the authorized user of those accounts.

Further, in most instances, access will be dependant upon the physical presentation of the appropriate token. Known security systems for limiting access to secured computer systems require that authorized user to possess and present a unique (but reproducible) token, such as a credit card or ATM card, and require the user to know and present a personal identification code, which is generally numeric in character.

Unfortunately, this almost universal system of access to secured systems has very serious flaws. First, access can be gained by anyone possessing the appropriate token and knowledge of the PIN linked to the token and ultimately to the user's account. The rapid increases in ATM crime and counterfeit credit card scares are testament to this point. Although token and code security systems do reduce the risk of unauthorized access, such security systems are nevertheless significantly susceptible to fraud. Because verification of user identity is based solely on data that can be easily reproduced and transferred between individuals, as opposed to data that is unique to and irreproducible from the user, such security systems must rely on both the diligence and the luck of the authorized user in maintaining this information as proprietary. The significant increase in ATM crime and counterfeit credit card scams are testament to the weaknesses of these systems, as are the plaintiff cries of the head of household who unwisely tendered both token and code to a less than thrifty friend or family member.

In addition to the significant ongoing risk of fraud, token and code security systems are frequently cumbersome for consumers to use. First, the consumer must physically possess the token in order to initiate access to the desired account. This inconvenience is greatly compounded by the fact that consumer often maintains a variety of active financial accounts, each issuing its own unique token and code. This requires the consumer not only to carry numerous tokens, but to remember each specific code for each specific token. Of course, a proliferation of tokens decreases the ability of the consumer to maintain the high degree of proprietary control upon which the token and code system relies.

Recently, various workers have attempted to overcome problems inherent in the token and code security system. One major focus has been to encrypt, variabilize or otherwise modify the PIN code to make it more difficult for an unauthorized user to carry out more than one transaction, largely by focusing on manipulation of the PIN access code to make such code more fraud resistant. A variety of approaches have been suggested, such introducing an algorithm that varies the PIN in a predictable way known only to the user, thereby requiring a different PIN code for each subsequent accessing of an account. For example, the PIN code can be varied and made specific to the calendar day or date of the access attempt. In yet another approach, a time-variable element is introduced to generate a non-predictable PIN code that is revealed only to an authorized user at the time of access. Although more resistant to fraud that systems incorporating non-variable codes, such an approach is not virtually fraud-proof because it still relies on data that is not uniquely and irreproducibly personal to the authorized user. Further, such systems further inconvenience consumers that already have trouble remembering constant codes, much less variable ones. Examples of these approaches are disclosed in U.S. Pat. Nos. 4,837,422 to Dethloff et al.; U.S. Pat. No. 4,998,279 to Weiss; U.S. Pat. No. 5,168,520 to Weiss; U.S. Pat. No. 5,251,259 to Mosley; U.S. Pat. No. 5,239,538 to Parrillo; U.S. Pat. No. 5,276,314 to Martino et al.; and U.S. Pat. No. 5,343,529 to Goldfine et al. all of which are incorporated herein by reference.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**