UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 5 | Issue 1 Article 16

2001

Eyeing the Future: Surviving the Criticisms of Biometric Authentication

Robyn Moo-Young

"Eyeing" the Future: Surviving the Criticisms of Biometric Authentication

I. INTRODUCTION

The problems associated with automated teller machine (ATM) cards and personal identification numbers (PINs) have been plentiful.[1] The stories include tales of stolen pin numbers, fraud, and identity theft.[2] In order to prevent these types of fraud, a move toward a more advanced, individualized technology known as biometrics has developed.[3] Biometrics is used for customer authentication and refers to the application of a certain trait or characteristic as an identifier and verification method.[4] There are several different identifiers that may be used in biometrics including, fingerprinting and hand geometry, voice recognition,

---

1. *See* Stephen Coleman, *Biometrics: Solving Cases of Mistaken Identity and More,* F.B.I. L. ENFORCEMENT BULL., June 1, 2000, at 9. Authentication security using an ATM card and PIN numbers is weak and often leads to fraudulent use of cards. *Id.*

2. *See* Kristen S. Provenza, *Identity Theft: Prevention and Liability,* 3 N.C. BANKING INST. 319, 319 (1999). *See also* Erin Joyce, *Fingerprints as Passwords: Twitching to Take Hold in Industry,* FUTURE BANKER, July 5, 1999, at 48 (stating that billions of dollars are lost each year due to stolen passwords and forged signatures).

3. Lisa Jane McGuire, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy,* 33 AKRON L. REV. 441, 444 (2000). McQuire's note addresses privacy, one of the major concerns associated with biometrics. *Id.* While many people believe that biometrics is intrusive, there are also many who have complete faith in it. *Id.* U.S. Senator Robert C. Byrd of West Virginia announced on September 7, 2000 that he planned on opening a Biometrics Fusion Center, which is to be run by the U.S. Army at the Benedum Airport Complex in Clarksburg, West Virginia. Blaine Mullins, *High-Tech Crime Fighting Facility Coming to North Central West Virginia,* STATE J. (Charleston W. Va.), Sept. 18, 2000, at 14. In the Fiscal Year 2001 Defense Department Appropriation Bill, Senator Byrd designated $25 million to advance the development and study of biometrics. *Id.*

4. McGuire, *supra* note 3, at 444-45. Biometrics is a promising method for banking because it provides security in addition to convenience. *See* Ferguson, *Putting a Finger on Security,* eWEEK, Sept. 25, 2000, at 16, 2000 WL 18179012. Ron Coben, executive vice president of Houston-based Bank United says that customers "have to have safety, they have to have security for the things they want to access, but they are not going to want to remember a unique code for everything in their life." *Id.*

retina and iris scans, signature recognition, and facial scans.[5] All of these identifiers are supposed to be unique to the individual, and systems using one or more of these identifiers are designed to protect privacy and prevent fraud.[6]

The biometric authentication process involves four steps.[7] First, a particular trait is scanned.[8] Second, those details are converted into a digital code.[9] Third, the code is stored in a database.[10] Fourth, when the customer wants to access her account, she is scanned again on site, and the information from the scan is compared to the code in the system.[11] Biometric technology eliminates carrying a card and reduces the possibility of fraud or theft.[12] Nonetheless, it has been greeted with criticism and doubt.[13]

This Note will compare the various methods used as well as the advantages and disadvantages of biometrics.[14] It will also examine biometric applications that are already implemented in our society and then address the feasibility, accessibility, and potential success of biometrics in the banking arena.[15] Finally, the Note will assess the balance between privacy and protection and the give and take relationship necessary to make this method of banking successful.[16]

---

5. Orla O'Sullivan, *Biometrics Comes to Life*, A.B.A. BANKING J., 31, 33-37 (Jan. 1997) .

6. Joyce, *supra* note 2, at 48. *See* David Green, *South Florida Sees New Breed of ATM, Credit Card Crooks*, MIAMI HERALD, Apr. 10, 2000, at A1 (discussing the fight between scam artists and police and addressing the high tech innovations which scam artists have created in order to "help themselves to billions of dollars in other people's cash each year"). *See also* O'Sullivan, *supra* note 5, at 31.

7. McGuire, *supra* note 3, at 445 (citing Bill Siuru, *Iris Recognition Systems*, ELECTRONICS NOW, Feb. 1999, at 41).

8. *Id.* at 445.

9. *Id.*

10. *Id.*

11. *Id.*

12. *See* Green, *supra* note 6, at A1. *See also* Joyce, *supra* note 2, at 48.

13. McGuire, *supra* note 3, at 472-74 (criticizing biometrics for invading customers' privacy). *See* Penny Lunt, *Advice From Top Technology Gurus*, A.B.A. BANKING J., 70, 74 (July 1996) (suggesting that biometrics is a "promising technology" but realizing that there are several privacy issues as well); *see also* Daniel Hall, *ATM Security Under Scrutiny*, A.B.A. BANKING J., 70, 72 (Nov. 1989) (indicating that biometrics is too costly).

14. *See infra* notes 69-207 and accompanying text.

15. *See infra* notes 17-68, 208-85 and accompanying text.

16. *See infra* notes 229-54, 264-85 and accompanying text.

II. BIOMETRICS USE TODAY

A. *Success*

Biometrics is not entirely new.[17] Several places in the United States and abroad have experimented with this advanced technology in ATMs.[18] In 1997, the Japanese began using retina scans for ATM access.[19] Chase Manhattan Bank uses voice recognition for customer identification.[20] After some trials, Chase found that 95% of consumers would prefer to use voice recognition and 80% would use fingerprinting.[21] Chase has also experimented with signature recognition.[22] In addition, as of 1997, Citicorp, Bank of America, Mellon Bank, Bankers Trust, and Chevy Chase Savings and Loan Association were all experimenting with fingerprint scanning.[23]

At Purdue University, the Purdue Employees Federal Credit Union uses finger printing at remote ATMs.[24] Also, self-service check-cashing machines, also known as Rapid Pay Machines, allow individuals who do not have an account with the bank to cash checks using facial recognition.[25] Facial scanning is

17. McGuire, *supra* note 3, at 445. Fingerprinting was used in the criminal context in the early 1900s. Vincent J. Gnoffo, *Requiring a Thumbprint for Notarized Transactions: The Battle Against Document Fraud,* 31 J. MARSHALL L. REV. 803, 803-04 (1998). Voice recognition can be traced back to the 1960s, and the idea of using the iris for identification can be traced to 1936, when an ophthalmologist named Franch Birch first came up with the idea. *Analysis: Biometric Identification, Using Physical Characteristics Such as a Voice Sample or Handprint to Identify a Person,* N.P.R.: TALK OF THE NATION, Sept. 1, 2000, 2000 WL 2145911 [hereinafter *Biometric Identification*]. This was a public radio interview with Dr. Jim Wayan, Direction of the National Biometric Test Center, with Ira Flatow as host. *Id.*

18. *See infra* notes 19-23 and accompanying text.

19. O'Sullivan, *supra* note 5, at 37.

20. *Id.*

21. *Id.*

22. *Id.*

23. *Id.*

24. McGuire, *supra* note 3, at 455 (citing *Technology: Banks' Future Security Could Be Built on Biometrics House Banking Panel Told,* B.N.A BANKING DAILY, May 21, 1998).

25. *Id.* at 455 (citing Helen Stock, *Firm Uses Biometrics to Serve the Unbanked,* AM. BANKER, Oct. 1, 1999, at 12).

also installed at the Pentagon to secure the computer network.[26] In addition, InnoVentry Corp, a biometrics developer based in California, has already installed 550 cash-checking kiosks that use face-scanning for customer authentication.[27] They have been installed at stores including Wal-Mart and McDonalds.[28] In Texas, Bank United set up ATMs using iris scanning in Kroger supermarkets in Dallas, Houston, and Fort Worth.[29] Foreign banks have also been experimenting with biometrics.[30] Banks in England and South Africa, for example, are utilizing technologies such as retina and thumbprint scans, rather than having customers carry bankcards.[31] In Australia, banks have over 1400 ATMs, which are unlocked using fingerprints.[32]

B. Biometric Use In Areas Other Than Banking

Biometrics is currently used in many areas other than banking.[33] It may serve the banks' best interest to observe the success of biometrics in these areas before embarking on their own biometric authentication ventures.[34] Hand scans are popular for gaining access to secure places, university dorms, apartment

---

26. O'Sullivan, *supra* note 5, at 37.

27. Ferguson, *supra* note 4, at 16.

28. *Id.*

29. *See* McGuire, *supra* note 3, at 455 n.80 (citing Leslie J. Nicholson, *Iris Scanning ATMs Coming Online Today,* DALLAS MORNING NEWS, May 13, 1999, at 10D).

30. Peter J. Howe, *The ATM's One Stop Future at the Corner Kiosk, You'll Be Able to Get Airline Tickets, Buy a Mutual Fund, Check the Sports Scores, and Oh, yeah, Grab Some Cash,* BOSTON GLOBE, Feb. 11, 1999, at G9.

31. *Id.*

32. O'Sullivan, *supra* note 5, at 33. In Australia, bank representatives bring a portable scanning device to the ATM. *Id.* The device plugs into the ATM machine and connects to the bank's server. *Id.* After scanning his finger, he gains admittance. *Id.* This method identifies who entered, as well as how long they stayed, thus "keep[ing] the representative honest." *Id.*

33. *See infra* notes 35-67 and accompanying text.

34. Mark Piper from BB&T expresses his concern that there is not yet a sound business case that is compelling banks to equip ATM machines with biometric devices. E-mail Interview with Mark Piper, BB&T ATM Management in Charlotte, N.C., Oct. 16, 2000 (on file with N.C. BANKING INST.) [hereinafter Piper Interview]. Without a sound business case, banks would be driving up the costs of both hardware and infrastructure without any payback. *Id.* By examining biometric success in other areas, banks can monitor public acceptance of this technology. *Id.*

buildings, and work places.[35] In addition, the hand scan when used in conjunction with a card has proven quite successful in what is known as the INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System) project.[36] Frequent travelers avoid long immigration lines at international airports in Los Angeles, Miami, Newark, New York City, Washington, San Francisco, Toronto, and Vancouver.[37] Passengers receive a card on which their hand scan information is held in a magnetic strip.[38] Using this card, passengers are able to bypass passport control personnel.[39] INSPASS travelers swipe their card, place their hand on a reader, and once verified, proceed ahead.[40] Approximately 50,000 passengers have enrolled in this service.[41] In addition to handling immigration at airports, fingerprint scanning and hand geometry are also used in border control projects.[42] Approximately 100,000 people cross the border into the United States each day in El Paso, Texas, making a quick and accurate identification ideal.[43]

In New York, Los Angeles, and Spain, fingerprint scanning

35. *Hand Scan Projects and Applications, at* http://www.hand-scan.com/projects_and_apps.htm (last visited Jan. 6, 2001). International Biometrics Group (IBG) is a consulting group that provides information and physical security concerns regarding biometrics to both public and private sector clients. Jennifer Kingson Bloom, *Tech Scene: Biometric ID Needs Careful Customer Sell*, AM. BANKER, May 24, 2000, at 15. It hosts several biometric websites such as www.finger-scan.com, www.facial-scan.com, www.iris-scan.com, www.retina-scan.com, www.hand-scan.com, www.voice.scan.com, and www.signature-scan.com. *Id.* IBG recently opened a store near Wall Street called "The BiometricStore," which aims to educate and familiarize people with biometrics. Deborah Bach, *Biometric Firm Takes Act to Street*, AM. BANKER, Feb. 6, 2001, at 1. It is the only independent biometric showroom in the world. *Id.*

36. *Hand Scan Projects and Applications, supra* note 35.

37. *Id.* Disney uses a similar process. *Id.* Season pass ticket holders can avoid long lines by going to a line which scans two of their fingers. *Id.* This promotes convenience and deters season pass ticket holders from sharing the pass with their friends. *Id.*

38. *Id.*

39. *Id.*

40. *Hand Scan Projects and Applications, supra* note 35. Currently in Israel, a hand scan project known as "Basel" is in its preliminary stages. *Id.* Basel will use both hand and facial scans to control access to a road between the Gaza strip and the West Bank. *Id.*

41. *Id.*

42. Coleman, *supra* note 1, at 12.

43. *Id.*

has been useful in ensuring that benefit recipients do not receive benefits more than once.[44] For example, in L.A. County, each time an individual applies for welfare benefits, his or her finger is scanned and then compared to millions of fingerprints already in the database.[45] If a match occurs, it is likely that that individual has tried to receive benefits under a different name.[46]

Furthermore, finger scanning is beneficial in personal computer security, allowing only the computer's owner to logon to the network and gain access to certain databases.[47] In Australia, Woolworth stores use finger scanning in order to verify the identity of employees and record their work time.[48] In Jamaica, finger scanning is used for voter registration.[49] Finger and hand scanning appear to be one of the most popular and successful methods of biometrics in areas outside of banking.[50]

Other methods in addition to hand and finger scanning play a beneficial role in society.[51] Face recognition has been used in several identification applications.[52] For example, in 1998, West Virginia was the first state to use facial recognition in connection with driver's license applications.[53] With the hopes of preventing people from obtaining a license under a false identity, West Virginia implemented facial recognition.[54] When people apply for a new license or replace lost or stolen ones, the system takes their photos and compares it to a previously recorded photo.[55] Also,

---

44. *Finger Scan Technology, at* http://www.biometricgroup.com/a_bio1/technology/cat_finger_scan.htm (last visited Nov. 5, 2000).

45. *Id.*

46. *See id.*

47. Mirian Leuchter, *Biometrics at the Crossroads,* BANK TECH. NEWS, Sept. 5, 2000, 2000 WL 17153571.

48. Eric Slater, *Not All See Eye to Eye on Biometrics; Iris and Fingerprint Scanners May Soon Come to the Corner Bank or Market, Critics Fear Loss of Privacy and Theft of Electric Identities,* L.A. TIMES, Apr. 28, 1998, at A1.

49. *Finger Scan Technology, supra* note 44.

50. *See supra* notes 35-49 and accompanying text.

51. *See infra* notes 53-67 and accompanying text.

52. *Id.*

53. Coleman, *supra* note 1, at 13 (citing Press Release, West Virginia Becomes First State to Issue Driver's Licenses Using Facial Recognition Technology (March 24, 1998)).

54. *Id.* at 13-14.

55. *Id.* at 13.

some PCs use facial scanning in lieu of a password for logging on to Windows.[56] Furthermore, the criminal arena utilizes facial scanning.[57] In 1988, the Lakewood Division of the Los Angeles County Sheriff's Department installed a system that can take a composite drawing or a video image of a suspect caught committing a crime and search that picture with the database of digitized mugshots on file.[58] The criminal arena not only uses facial scanning but also voice recognition.[59] Voice recognition is also used to track the identity of parolees who are under home incarceration.[60] Therefore, a parolee could be tracked using a simple telephone call.[61]

Biometrics using the human eye also has a multitude of applications outside of the banking scene.[62] Retina scanning allows employees to gain physical access to certain highly sensitive work areas, rooms in military installations, and power plants.[63] Like facial and voice recognition, iris scanning has been used for prisoner identification purposes.[64] In Florida and Pennsylvania, prisons use IriScan, a leading manufacturer of iris scanning devices.[65] Over 9,000 prisoners are scanned into the database, and each time a prisoner is transferred or released, he is scanned again.[66] This helps the prisons keep track of who leaves and who enters.[67] Evidently, biometric authentication has been quite advantageous.[68] Its applications not only serve protection and

56. Leuchter, *supra* note 47. Microsoft has structured a deal with I/O Software Inc. to include biometrics into the future version of Windows operating system. *Id.* This I/O technology "works on any biometric data: fingerprint, hand and face geometry, iris and retina scans and vocal patterns." *Id.*

57. *See infra* note 58 and accompanying text.

58. Coleman, *supra* note 1, at 13.

59. *See infra* note 60 and accompanying text.

60. *Voice Scan, at* http://www.voice-scan.com (last visited Jan 6, 2001).

61. *See id.*

62. *See infra* notes 63-68 and accompanying text.

63. *Retina Scan Applications, at* http://www.retina-scan.com/retina_scan_applications.htm (last visited Jan. 6, 2001).

64. *Iris Recognition in Action, at* http://www.iris-scan.com/iris_recognition_applications.htm (last visited Jan. 6, 2001).

65. *Id.*

66. *Id.*

67. *Id.*

68. *See supra* notes 35-67 and accompanying text.

security purposes, but also aid in convenience and efficiency. While it has been successful in achieving widespread use in other areas, whether biometrics will succeed in the banking industry as well remains uncertain.

III. BIOMETRIC AUTHENTICATION METHODS

A. Retina and Iris Scans

Retina scanning maps the vein pattern on a customer's retina, which is the innermost part of the eye.[69] A beam of light reflects off of the retina, and the blood vessel pattern is then transformed into a digital code.[70] Iris scans are similar to retina scans. They map the colored part of the eye, known as the iris.[71] The database compares several different identifiers, known as discriminators.[72] These include the corona, pits, filaments, crypts, striation, radial furrows, and other structures.[73] A special video camera at the ATM machine takes a high-resolution picture of the iris and compares it to the iris in the database.[74] Although there are many identifiers, a iris match can be made in as quickly as two to three seconds, and an accurate image can be taken from as far as three feet away.[75] In addition, iris scans can be taken through

69. John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns - Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 102-3 (1997).

70. *Id.*

71. O'Sullivan, *supra* note 5, at 31.

72. McGuire, *supra* note 3, at 448 n.38 (citing John D. Woodward, Comment, *Biometrics Offers Security But Legal Worries, Too*, AM. BANKER, Aug. 23, 1996, at 11 (citing Kurt Loft, *Eye on Tomorrow; The Information Obtained From a Simple Scan of Your Eye's Iris Could Replace the Need for ATM Cards and the PINs That Go With Them*, TAMPA TRIB., July 26, 1999, at 4)).

73. *Scanner "Reads" Iris Pattern*, A.B.A. BANKING J., 61 (April 1999); McGuire, *supra* note 3, at 448 n.38 (citing Loft, *supra* note 72).

74. *See* McGuire, *supra* note 3, at 448 n.41 (citing Ashley Dunn, *The Cutting Edge; The Password is Biometrics; High-Tech Identification Systems are Moving Into Corporate and PC Worlds, Offering Log-On Security in the Blink of an Eye or the Tap of a Finger*, L.A. TIMES, Dec. 7, 1998, at C1).

75. *Id. See Iris Recognition: The Technology, at* http://www.iris-scan.com/iris_technology.htm (last visited Nov. 5, 2000). Iris scanning systems can locate the iris within about a quarter of a second. *Id.* The image of the iris is converted into an algorithm, known as the Iris Code, and that can be generated in one second. *Id.* Furthermore, hundreds of thousands of records can be searched per second in the

contact lenses and most glasses.[76] If a match results, payment approval or access is granted.[77]

Iris and retina scanning, however, do have minor drawbacks.[78] Because the retina is located in the back part of the eye, retina scans need perfect alignment of the eye to reach it.[79] In addition, retinal scans often fail because the eye can change during pregnancy.[80] While iris scans are said to be the most promising of biometric identification methods, they do require much more computer storage memory than fingerprints.[81]

Because other methods such as fingerprinting and voice recognition may encounter difficulties due to weather, emotion, vandalism, and potential for fraud, iris scans have shown to be the most promising of methods.[82] A customer does not have to touch anything; the customer simply holds her eye up to a machine.[83] In

---

database. *Id.*

76. *Scanner "Reads" Iris Pattern*, *supra* note 73, at 61; McGuire, *supra* note 3, at 448 n.40 (citing Dunn, *supra* note 74). Designer contacts may pose a difficulty because some have fake iris patterns on them. *Biometric Identification*, *supra* note 17. Dr. John Daugman, professor in the computer laboratory of Cambridge University in the United Kingdom, noted that there are ways to detect such fake patterns. *Id.*

77. *Scanner "reads" Iris Pattern*, *supra* note 73, at 61.

78. *See infra* notes 79-81 and accompanying text.

79. O'Sullivan, *supra* note 5, at 37. In 1997 Japan was already using retina scans for ATM machines. *Id.* Certain Asian cultures prefer eye scanning to fingerprinting because they are against the physical contact involved with such systems as fingerprinting. *Id.*

80. Kathryn Leonard, *Biometrics: Digitize This*, POPULAR SCIENCE, Oct. 2000, at 20.

81. McGuire, *supra* note 3, at 448 n.42 (citing Rajiv Chandrasekaran, *Brave New Whorl; ID Systems Using the Human Body Are Here, But Privacy Issues Persist*, WASH. POST, Mar. 30, 1997, at H1). Of the biometrics methods, fingerprinting requires the least amount of computer storage while iris scanning requires the most. *Id.*

82. Hall, *supra* note 13, at 72. Phil Britt, *High-Tech Identification Systems Come of Age: Biometrics in Banks; Includes Related Article on Privacy*, AM. COMTY. BANKER, June 1998, at 22 (stating that fingerprinting has problems with dirty hands and weather). *See also* Woodward, *supra* note 69, at 107 (starting that voice recognition has trouble with background noise, illness, and emotion). *But see* Hall, *supra* note 13, at 72 (stating that if vandals painted over the retina/iris scanning lens, the lens would be useless).

83. *See* E-mail interview with Becky McCloskey, Wachovia, Charlotte, N.C. (Oct. 24, 2000) (on file with N.C. BANKING INST.) [hereinafter McCloskey Interview]. McCloskey believes that iris scanning would be great because it is accurate and not very intrusive to the customer. *Id.* It is not difficult for the customer to use and does not have too high of a failure rate, which makes customers frustrated. *Id.*

addition, this method is not susceptible to fraud since a photograph cannot be substituted for the real eye.[84] The technique uses physiological response to light and natural pupillary oscillation, which cannot be replicated, by use of a photo.[85] The video camera scans the iris several times and verifies that the pupil is in fact moving.[86]

Iris scans are more reliable than fingerprinting because they contain more discriminators or identifiers.[87] For instance, a finger has about thirty-five identifiers, while an iris scan has about 266.[88] Because the 266 identifiers must match up, there is much less room for error.[89] According to one specialist, "[t]he great strength of iris recognition is a really astronomically low false match probability. In fact, in all of the published scientific tests of these algorithms, there's never been a single documented false match."[90] Additionally, at two to three seconds, iris scans are fast as well as accurate.[91] Furthermore, the structure of the iris is determined before birth and does not change over time, with the exception of possible coloration.[92] The scanning device can also discern between the left and the right eye.[93] While retina scans have proven to have some difficulty with differentiating between identical twins, there is an insignificant likelihood that someone

84. McGuire, *supra* note 3, at 448 n.41 (citing Bill Siuru, *Iris Recognition Systems,* ELECTRONICS NOW, Feb. 1999, at 41).

85. *Id.*

86. *Id.* (citing *How the Eyeball Scanner Will Know It's You,* ST. LOUIS POST-DISPATCH, June 5, 1996, at 5C).

87. *Id.* at 448 n.38.

88. *Id.* (citing Loft, *supra* note 72 (reporting that a fingerprint has about thirty-five identifiers, while an iris scan has about 266)).

89. *See id.*

90. *Biometric Identification, supra* note 17 (quoting Dr. John Daugman, a professor in the computer laboratory at the University of Cambridge in the United Kingdom). Dr. Daugman's research and patents provide the primary basis for iris recognition technology. *See Iris Recognition: The Technology, supra* note 75.

91. *Iris Recognition: The Technology, supra* note 75. The odds of two different iris scans retrieving the same IrisCode are very small at 1 in 10^{52}. *Id.*

92. *Biometric Identification, supra* note 17. Iris formation occurs before birth, usually around the third month of gestation. *Id.*

93. *Scanner "reads" Iris Pattern, supra* note 73, at 70. The left and right eye are genetically the same, but they have different irises. *Id.* Therefore, an iris scan can differentiate between the left and the right eye. *See id.* "There is a statistically insignificant likelihood of someone else, even a family member, sharing your Iris pattern." *Id.*

else, including a family member, will have the same iris pattern.[94]

It also seems doubtful society would have the same concerns regarding retina/iris scanning as thumb printing because there is less likelihood of an eye being gouged out as a thumb being removed. In addition, an early survey indicated customer preference for iris scanning, with 91% choosing iris identification over PINs or signatures.[95]

B. Other Methods

1. Fingerprint and Hand Geometry

Finger scanning technology examines the unique characteristics of fingerprints including whorls, arches, loops, and ridges, once a fingerprint has been scanned into a large database.[96] Hand geometry is similar to fingerprinting but measures the length, width, and height of the hand and fingers.[97]

There are two basic types of finger scanning technologies available – identification systems known as automatic fingerprint identification systems (AFIS) and verification systems.[98] Identification systems use a fingerprint to identify the customer.[99] On the other hand, verification systems perform what is known as a "one-to-one verification," which entails comparing an on-site fingerprint to a pre-existing fingerprint already in the database.[100]

---

94. *Scanner "Reads" Iris Pattern, supra* note 73, at 61.

95. *Id.*

96. *Finger Scan Technology, supra* note 44.

97. Woodward, *supra* note 69, at 105.

98. *Finger Scan Technology, supra* note 44. Verification system units, which use a one-to-one process can cost anywhere from a couple hundred dollars to a couple thousand dollars. *Id.* However, this cost is expected to drop with the entrance of big companies such as Sony and Motorola into the biometric industry. *Id.* Identification systems, like AFIS, provide a one-to-many process. *Id.* The fingerprint image of the person being scanned is being compared to all the images stored in the system. *Id.* If the database is large, the response time will be slower and the cost will be much greater. *Id.* Forensic applications are generally more expensive then civil because rolled prints contain much more data than simply a flat image. *Id.*

99. *Id.*

100. *Finger Scan Technology, supra* note 44.

There are two types of AFIS applications – forensic and civil.[101] Forensic applications examine a rolled image of all ten fingers.[102] Civil applications examine a flat image of a finger or several fingers.[103] In contrast to the AFIS method, verification systems look at the flat image of a finger and perform a one-to-one verification process in a matter of seconds.[104]

The three main types of finger scanning capture devices are optical scanners, ultrasound scanners, and chip-based sensors.[105] AFIS systems primarily use optical scanners, whereas verification systems may use any of the three types.[106] ATMs would most likely use verification applications because banks want to ensure that users are who they say they are.[107] During an optical scan, when customers wish to gain access to their account at an ATM machine, they simply press a finger onto a touchpad, and that fingerprint is compared to the one in the system.[108] Researchers have also looked into ultrasonic scanning of a fingerprint.[109] Using ultrasound technology, a customer places a finger on a glass surface and feels vibrations as an ultrasonic image is taken.[110] Because sound is used rather than an optical image, a dirty finger

101. *Id.* AFIS software providers are Printak, SAGEM, NEC, Cogent, and TRW. *Id.* AFIS forensic hardware vendors are Printak, Identix, and digital biometrics. *Id.* AFIS civil hardware vendors are Identix, Digital Biometrics, Cross Match, Identicator and TRW. *Id.*

102. *Id.* Forensic applications, which use rolled images, aid police because they provide more data. *Id.* They can track demographic information as well as attach police tracking data. *Id.*

103. *Id.* Identification applications generally take a couple of minutes to process, depending on the size of the database. *Id.*

104. *Id.*

105. *Finger Scan Technology, supra* note 44. Although "optical" seems to imply some relationship to the eye, it does not in this case. *Finger-Scan Technology: Optical, Silicon, Ultrasound, at* http://www.finger-scan.com/finger-scan_technology.htm (last visited Jan. 6, 2001). An optical scan in essence takes a flash photograph of the finger and using the dark ridges and light valleys of the print, converts it into a digital signal. *Id.*

106. *Id.*

107. *See id.*

108. *Id.* Some of the vendors who produce optical scanning devices include: American Biometric Company, Identix, Identicator, BAC, SAC, Cross Match, and Digital Persona. *Id.*

109. *Finger Scan Technology, supra* note 44. UltraScan, which is manufactured by Kodak is the predominant vendor for ultrasonic devices. *Id.*

110. *Id.*

is irrelevant.[111] In the third alternative, using chip-based sensors, customers place their finger directly onto silicon chips.[112] The silicon sensor acts as one plate of a capacitor, while the finger acts as another plate.[113] The capacitance, or the electric charge between these two plates, is converted into an eight-bit grayscale digital image.[114] Unlike an optical scan which relies primarily on darkness and light, silicon chip-based scans focus more on variation.[115] Because each silicon chip is composed of very small rows and columns - each of which hold 200 to 300 lines - a silicon or chip-based scan is often very accurate and detailed.[116]

The major drawback to fingerprinting is that weather, oils, cuts, and germs can impact its success.[117] If the touchpad gets wet, a customer is likely to encounter problems.[118] A representative of a manufacturer of ATMs reported that "person after person putting their finger on the same spot created a real problem for the scanner."[119] The physical condition of the user's fingers have an effect on accuracy.[120] Some suggest that stone workers, bricklayers, and even gardeners may have trouble using fingerprinting because they do a lot of work with their hands, making their fingers shiny

111. *Id.*

112. *Id.* Silicon chip-based vendors include: Thomson-CSF, Infineon, ST Microelectronics, Authentec, Veridicom and Who?Vision. *Id.*

113. *Finger-Scan Technology: Optical, Silicon, Ultrasound, supra* note 105. A capacitor is defined as an electric circuit element used to store charge temporarily, consisting in general of two metallic plates separated by a dielectric or nonconductor. THE AM. HERITAGE DESK DICTIONARY 155 (1981).

114. *Finger-Scan Technology: Optical, Silicon, Ultrasound, supra* note 105.

115. *Id.*

116. *Id.*

117. Woodward, *supra* note 72, at 105 (stating that natural oils in fingers and sweat may cause the finger to adhere to the touchpad)). *But see Finger Scan Technology, supra* note 44. Because ultrasonic scanning involves the use of sound to capture the finger image, ultrasounds do not need perfectly clean fingers. *Id.* It will even work if the customer is wearing a thin latex glove. *Id.*

118. McGuire, *supra* note 3, at 448 n.42.

119. Leuchter, *supra* note 47 (quoting Mark Radke of Diebold, Inc.). One of the major drawbacks of optical scanning of fingers is that with repeated use, dirt and residue can build, thus interfering with the scan. *See id.* In addition, latent prints, prints left over from previous users, may cause two different prints to be scanned. *Finger-Scan Technology: Optical, Silicon, Ultrasound, supra* note 105. Also, the coat on the plate may wear after some time. *Id.*

120. *See infra* notes 121-22 and accompanying text.

and weathered.[121] Other potential problems include if a customer has a cut; the fingerprints will not match up.[122] Also, fingerprints can be forged by rubber stamps.[123] In addition, skeptics of biometrics argue that fingerprinting has "Orwellian, if not downright, criminal connotations."[124] A concern has also been expressed that fingerprinting is a breeding ground for germs[125] and that fingerprinting will lead to the dismemberment of fingers to gain access into a customer's account.[126]

There are, however, advantages to using the fingerprint method as well. One of the advantages of fingerprinting is its ability to detect changes in temperature.[127] Therefore, if someone forces a customer up to a machine and demands that the customer take out money, the scanner recognizes a distressed finger and will not permit access to the account.[128] It will also alert the bank there is trouble.[129] Another advantage of fingerprinting and hand geometry is that they use small amounts of computer storage memory.[130] Some systems may even compensate for an injured or distorted fingerprint by allowing a customer to enter more than one fingerprint into the system.[131] Consequently, if one finger is

121. *Biometric Identification, supra* note 17.

122. *But see* McGuire, *supra* note 3, at 448 n.42 (citing Rajiv Chandrasekaran, *Brave New Whorl; ID Systems Using the Human Body are Here, But Privacy Issues Persist,* WASH. POST, Mar. 30, 1997 (suggesting that the system can compensate for injuries by using another finger)).

123. Leonard, *supra* note 80.

124. O'Sullivan, *supra* note 5, at 31 (pointing out, that despite the criminal undertones, a 1997 nationwide survey by Columbia University found that 83% of people supported the use of fingerprinting and do not feel that they are being treated as criminals). In discussing biometrics with their customers, banks are urged not to use the word "fingerprint" because doing so may trigger law enforcement connotations. Bloom, *supra* note 35, at 1.

125. McGuire, *supra* note 3, at 449 n.47.

126. David Hoffman, *A Thumbprint I.D. Could Cost Some Thumbs,* BUS. WK., Apr. 3, 2000, at 5.

127. *See* Teresa Dixon Murray, *Show & Tell Latest ATM Marketing Philosophy: You'll Come for Money, Stay for Ads,* HARRISBURG PATRIOT, (Harrisburg, Pa.), May 10, 1999, at B3. Fingerprint technology requires a finger to be at body temperature. *Id.*

128. Joyce, *supra* note 2, at 48.

129. *Id.*

130. Woodward, *supra* note 69, at 106.

131. *Id.* at 448 n.42 (citing Joe Ward, *Ex-Louisvillian Pioneers Access to Computers by Fingerprint,* COURIER-JOURNAL (Louisville, Ky.), May 30, 1999, at 1E).

cut or injured, a customer can simply use another.

2. Voice Recognition

Voice recognition takes an acoustic signal of a person's voice and converts it into a digital code which is then stored in a database.[132] The user records a certain phrase, usually repeating it several times.[133] The system then measures tone, pitch, and voice cadence.[134] However, emotions, illness, and stress can all affect a successful voice authentication. [135] Also, background noises may lead to an unsuccessful recognition.[136]

Voice recognition is useful, however, because customers can gain access to their accounts from distant places.[137] Customers can call from anywhere in the world and authorize a transfer of funds or inform of their balance.[138] It does not require that a customer be present at the bank in order to gain access to customer accounts.[139] Voice recognition may be valuable in other aspects of banking but not necessarily ATM use.

3. Signature Recognition

Signature recognition does more than just compare two signatures. [140] It compares the shape and speed of the letter strokes, and looks at the number of times a pen leaves the surface.[141] In addition, it recognizes the speed at which the signatures are made.[142] PenOp is a software company that has

132. Woodward, *supra* note 69, at 107.

133. *Id.*

134. Britt, *supra* note 82, at 22. Cadence is the inflection or change in pitch and tone of the voice. AM. HERITAGE DESK DICTIONARY 147 (1981).

135. Coleman, *supra* note 1, at 9; Woodward, *supra* note 69, at 107 (1997).

136. Coleman, *supra* note 1.

137. O'Sullivan, *supra* note 5, at 31. Unlike finger scanners which need special readers, voice recognition can work right over the phone. *Id.*

138. *Id.*

139. *Id.*

140. Woodward, *supra* note 69, at 107.

141. *Id.*

142. *Id.* at 105.

made special pens that are used for signature recognition.[143] The process mainly has been used for electronic documents and entails attaching a pad to a computer, signing the pad with a stylus, and having it verified.[144] An independent consultant for Chase Manhattan bank states that "it can tell how fast you write, how you dot your i's and cross your t's." [145] While technology like signature recognition is often believed to be expensive, it has in fact become quite affordable. The PenOp software is now available for $99 per computer.[146] PenOp software targets e-signatures or signatures over the computer and internet. Signature recognition, however, has also been suggested for ATM use.[147]

In regard to handwriting systems, it has often been said that "no one ever signs exactly the same way twice."[148] Thus, some companies rationalize that a perfect match is a sure sign of forgery.[149] In order to offer further security, most handwriting systems require a customer to input several signatures into the system.[150] However, if no two signatures are the same, putting several signatures in the system is not likely to significantly increase the success rates. Also, signatures are often affected by injuries to the hand.[151]

One of the advantages of handwriting and signature recognition, however, is that it is not intrusive. Unlike retina scans and fingerprints, handwriting itself neither divulges any personal information nor has the potential to expose medical information.[152]

---

143. Leonard, *supra* note 80. PenOp, the leading provider of e-commerce signature technology was founded in 1990. *Id.* PenOp's software allows people to create a legally binding signature over the internet and through other electronic documents. *PenOp Company Overview, at* http://www.biometricgroup.com/a_bio1/vendor/penop.htm (last visited Nov. 8, 2000).

144. Leonard, *supra* note 80; Christopher B. Woods, *Commercial Law: Determining Repugnancy in an Electronic Age: Excluded Transactions Under Electronic Writing and Signature Legislation*, 52 OKLA. L. REV. 411, 417 (1999).

145. O'Sullivan, *supra* note 5, at 31.

146. Leonard, *supra* note 80.

147. Woods, *supra* note 144, at 417.

148. Leonard, *supra* note 80.

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

4. Facial Geometry

Facial scanning is also a technique that utilizes an individual's physical characteristics.[153] During the process, an image of a customer is taken and stored in a database.[154] The scanning device then identifies customers by bone structure.[155] A customer stands in front of a camera, which takes a picture of the customer's face and then compares the face's bone structure to the one that had been previously stored in the database.[156] In addition to the bone structure method, there are also several variations of facial scanning. For instance, one method known as feature analysis looks at geometric points.[157] This analysis examines the position of the eyes, the tip of the nose, the tip of the chin, and other points in order to create a template.[158] Once a face is scanned on site, the scan is compared to the composed template that is already in the system.[159] Similarly, automatic face processing (AFP) examines the distance between features, including between the eyes, to the end of the nose, and between the corners of a mouth.[160]

Another variation of facial scanning is neural network technology.[161] Humans are able to recognize other people. When

153. Christine Malamanig, *Check-Cashing Catches on at Bakersfield, Calif. Area Convenience Stores,* BAKERSFIELD CALIFORNIAN, Sept. 25, 2000, 2000 WL 27468711. Four facial-scanning, check-cashing machines, similar to ATM machines, are used in Circle K convenience stores in Bakersfield and Wasco, California. *Id.*

154. *Id.*

155. *Id.*

156. *Facial Scan Technology: How it Works, at* http://www.facial-scan.com/facial-scan_technology.htm (last visited Nov. 5, 2000).

157. *Id.*

158. Telephone Interview with William Parra, Emerging Technology, Bank of America, Charlotte, N.C, (Nov. 3, 2000) [hereinafter Parra Interview].

159. *Id.* Visionics is a leading company in facial recognition technology. *Facial Scan Technology: How it Works, supra* note 156. It uses Local Feature Analysis (LFA), which utilizes several features from different areas of a face and looks at their location. *Id.* In addition, it can accommodate for slightly different angles. *Id.* For example, if a person moves his mouth, the technology anticipates and compensates for the fact that the areas around the mouth will also be affected. *Id.*

160. *Facial Scan Technology: How it works, supra* note 156. AFP, while not as advanced as the other facial scanning technologies, does have the advantage that it can work rather effectively in dimly lit situations. *Id.* Most of the other facial scanning methods need a well lit situation. *Id.*

161. *Id.* Neural net technology is currently available and favored by a company

we see people our brain reacts, and we make a connection between the person standing before us and an image of that person we have stored in our brain.[162] Neural network technology attempts to look at the way our brain processes that recognition and tries to recreate this process using a computer.[163] Essentially, it makes computers work like the human brain.[164]

Finally, eigenfaces are another type of facial scan.[165] "Eigenface," meaning "one's own face," is a technology, patented by MIT, that looks at two-dimensional, gray-scale images of a person's face.[166] Each eigenface highlights a different characteristic using gray tones, but when all the individual eigenfaces are combined, a complete image is created.[167] Each face takes approximately 100 to 125 eigenfaces to create.[168] Customers' eigenfaces are converted to a series of numbers and then stored in a template.[169] This template is compared to customers' on site template formation.[170] The amount of variance between the two determines whether access is granted.[171]

Potential weaknesses of facial scans are the difficulties with identical twins and look-alikes.[172] In addition, when First Union experimented with this method for check cashing machines, one problem it encountered was customers not standing in the range of the camera.[173] However, because facial scanning uses bone structure as a basis for verification, the system will still recognize customers who have gained weight or altered their hairstyle.[174]

---

called Miros. *Id.*

162. Parra Interview, *supra* note 158.

163. *Facial Scan Technology: How it Works, supra* note 156.

164. *Id.*

165. *Id.*

166. *Id.* Eigenface technology presents the best results in well-lit situations, capturing frontal images. *Id.*

167. *Id.*

168. *Facial Scan Technology: How it works, supra* note 156.

169. *Id.*

170. *Id.*

171. *Id.*

172. Coleman, *supra* note 1, at 9.

173. Telephone interview with Ralph Perry, ATM Management, First Union, Charlotte, NC (Oct. 16, 2000) [hereinafter Perry Interview].

174. Malamanig, *supra* note 153. *But see,* Perry Interview, *supra* note 173 (suggesting that hairstyles and weight gain may affect recognition).

Using neural net technology also has the advantage of differentiating between twins.[175] After some time, people can often recognize the difference between identical twins.[176] Being able to replicate this process solves the identical twin problem.[177]

5. Other Methods in Preliminary Stages

In addition to the methods mentioned above, researchers are examining odor recognition where a person's natural body odor is used as an identifier.[178] Next, because it is less invasive, they are also studying keystroke recognition.[179] People strike keys on a keyboard differently. For example, keystrokes vary in speed, pressure, and more.[180] Finally, researchers are analyzing a person's walk, by measuring the person's gait.[181] One editor joked that banks would soon be using DNA ATM machines, which would involve spitting into a tiny slot.[182] Banks, however, have not taken biometrics use this far. As for odor, keystroke, and gait recognition, these methods are still in their preliminary stages.[183]

---

175. Parra Interview, *supra* note 158.

176. *Id.*

177. *See id.*

178. Parra Interview, *supra* note 158. *See also* Benny Evangelista, *Your Body is Your Password/Biometrics Lets Machines Recognize Specific Humans by Their Physical Traits,* SAN FRAN. CHRONICLE, Feb. 21, 2000, at B1 (stating that biometric products using body odor have not been profitable).

179. Parra Interview, *supra* note 158.

180. *Id.*

181. *See* Evangelista, *supra* note 178, at B1. Body odor and walk are two methods that have made little profits. *Id.*

182. Bill Schadewald, *Editor Denies That He's Cloned: Expectorate The Unexpectorate,* BUS. J. OF PORTLAND, Mar. 17, 2000, at 66. Schadewald jokes that Bank of Northern Hemisphere is making an ATM machine, whose DNA testing device breaks down the user's saliva into basic strands and then compares it to the user's DNA that is already on record in the database. *Id.* "We're confident that this new DNA testing will provide proof positive 100 percent of the time – as long as O.J. Simpson doesn't use the ATM." *Id.* DNA is defined as deoxyribonucleic acid, which contains an individual's genetic make-up. THE AM. HERITAGE DESK DICTIONARY 276 (1981). DNA is used for paternity test, cloning, finding missing children, and evidence in cases. GEORGE B. JOHNSON ET AL., BIOLOGY: PRINCIPLES AND EXPLORATIONS 203-11 (1998).

183. Parra Interview, *supra* note 158.

IV. BENEFITS OF BIOMETRIC IDENTIFICATION

A. Convenience

With biometrics, customers are not required to carry cards and thus do not run the risk of losing them or having them stolen.[184] Biometric information cannot be stolen by a discreet observer, and customers do not have to worry about forgetting their PINs and passwords.[185] It is a convenience for customers as well as a tool to reduce fraud.[186] Some may expect that customers would not want to relinquish something so personal as a unique trait, but according to one observer, "Anything that saves the information-overloaded citizen from having to remember another password or personal identification number comes as a welcome respite."[187] This enthusiasm was shared by another who stated "the fewer cards I need to carry in my wallet, and the fewer pin numbers I need to remember the better!"[188]

B. Heightened Accuracy and Reduction of Theft

Biometrics will decrease identity fraud and scams.[189] In Chicago, a woman was forced at gunpoint to take money out of her bank account at her ATM.[190] She was then shot five blocks away from the machine.[191] Because customers do not have to carry a card around and because certain biometrics methods can detect temperature change and distress, they would not have to worry as much about this all too common incident from occurring again.[192] Incident rates for scams and identity fraud are increasing every

184. *See infra* notes 185-88 and accompanying text.
185. Leuchter, *supra* note 47.
186. *See infra* notes 188-207 and accompanying text.
187. O'Sullivan, *supra* note 5, at 39.
188. McCloskey Interview, *supra* note 83.
189. *See* Joyce, *supra* note 2, at 48.
190. Hall, *supra* note 13, at 70.
191. *Id.*
192. Joyce, *supra* note 2, at 48.

day.[193] According to some, in the fight against scam artists, "[c]ops are losing [a]nd so are consumers."[194]

While technology such as biometrics can safeguard against some scams, technology can also aid the scam artists in their quest to pilfer money from innocent ATM users. For example, some scam artists use what is known as a "skimmer."[195] This device reads the magnetic strip of credit cards, ATM cards, and debit cards, and records the mathematical logarithm, which is necessary in order to gain access to the account.[196] Formerly bulky and cumbersome, these machines are now much smaller and can hold many accounts.[197] Because debit cards can also be used as an ATM card, customers run the risk of having their card skimmed when they pay for a meal or an item and thus, the perpetrators gain access to their account.[198] In addition, having a card in general leads to the possibility of having it stolen, and once stolen, the ATM card may be easily skimmed.[199] The solution lies in biometrics. The key to solving this problem is using technology more advanced than that employed by scam artists and by doing so, staying one step ahead of them, rather than one step behind.

193. Green, *supra* note 6 (noting that more than 2,000 Americans are the victims of identity theft each week, amounting to over $2 billion a year in losses).

194. *Id.* One scam, popular in Florida, entails the scam artists inserting a sleeve of tape into an ATM card slot. *Id.* This prevents the card from being spit back out and leads innocent customers to believe that they have mis-entered their pin number. *Id.* Beforehand, the scam artists place a sign on the machine instructing customers to enter their pin number several times or until the machine responds. *Id.* They pose as other customers in line and while customers repeatedly enter their pin numbers, the scam artists "shoulder surf," waiting to catch a glimpse of the pin number. *Id.* Sometimes, posing as fellow customers, they urge the innocent to follow the signs instructions and when it proves fruitless, they suggest coming back later. *Id.* When the coast clears, the scam artists retrieve the card out of the slot using tweezers, having successfully stolen the card and the pin number. *Id.*

195. *Id.* Skimmers can be assembled by using electronic parts that are bought at any electronics store.

196. *Id.* Many credit cards and debit cards are "skimmed" at restaurants. *Id.* Investigators across the country found that there were organized groups of wait staffers, which ripped off their own customers at restaurants. *Id.*

197. *Id.* While they used to be as large as a book and could only hold a dozen numbers, skimmers are now as small as a beeper and can hold hundreds of account numbers.

198. Many times, when debit cards are used as credit cards, customers are not asked for their pin number. Therefore, access to a debit card holder's account is possible.

199. Green, *supra* note 6.

The outdated ATM cards are susceptible to scam artists.[200] Because customers do not have to insert a code or punch in a number, iris scanning may be the solution.[201]

To further reduce fraud, fingerprinting has already been used for check cashing by non-account holders.[202] Customers provide a fingerprint in order to cash a check.[203] If the check clears, then nothing is done.[204] But, if the check does not clear, the bank gives the check and the fingerprint to law enforcement.[205] This protects the general public and customers in the long run by not just avoiding fraud, but taking action against it. Financial institutions in California that used this method of checking noted an 85% decrease in losses from check fraud.[206] In Charlotte, NC, First Union noted a 45% decrease in check fraud losses during its first year using fingerprinting.[207]

V. CONCERNS PREVENTING CURRENT WIDESPREAD ADOPTION OF BIOMETRIC IDENTIFICATION

There are several concerns that must be assuaged before biometric methods will be adopted for customer banking.

A. Lack of standardization around a particular method

Banks do not want to invest time and money into a

200. *Id.*

201. *Id.* A California company offers another solution--"modeling" software, which examines a customer's spending habits. *Id.* If any unusual pattern appears, it alerts the company and consequently, the customer. *Id.*

202. McGuire, *supra* note 3, at 454-55. Customers are asked to provide a fingerprint at the inception of an account and in order to cash a check. Some retail stores even use fingerprinting when a customer wants to write a check for a purchase in order to verify that the shopper is who he/she says he/she is. *Id.*

203. *Id.* at 455 n.71 (citing *Colorado Banks to Fingerprint to Stem Fraud,* A.C.L.U NEWS WIRE, July 30, 1996, *available at* http://www.aclu.org/news/w073096a.htm (last visited Sept. 9, 1999).

204. *Id.* (citing *Banks Increasingly Turn To Fingerprints,* A.C.L.U NEWS WIRE, Jan. 8,1997, *available at* http://www.aclu.org/news/w010897b.htm (last visited Sept. 3, 1999)).

205. *Id.*

206. *Id* at 444, n.13 (citing *Check Fraud: Check Fraud Losses Rising Rapidly Despite Banks' Growing Use of Technology,* B.N.A. DAILY, May 2, 1997, at D2.)

207. *Id.* (citing Britt, *supra* note 82, at 22).

technology that may not become an industry standard. They are apprehensive about integrating this technology into their ATMs because there is currently no external force that is driving them to abandon use of ATM cards.[208] One banker reports that banking officials will not focus much of their attention on biometrics until a sound business case is presented.[209] He states, "Until and unless every other card issuer moves to a standard biometric, we still have to equip ATMs with card readers. And until and unless every other ATM deployer moves to a standard biometric, we will still have to issue ATM cards with PINs to every ATM-using customer. By employing biometrics, we would simply be driving up our ATM hardware costs and infrastructure costs without any corresponding payback."[210] Some banks such as First Union are waiting for other banks to serve as pioneers before they invest their money in biometric ATM machines.[211] Apparently, banks need an external force to indicate that biometrics will be both acceptable and successful before they can justify the investment. The question then becomes who will make the first leap. Because many statistics have shown positive feedback and because biometrics deters fraud and crime,[212] it is not something that should be abandoned so quickly.

B. Costs

Such advanced technology might be expected to come with a hefty price tag, but prices for biometrics equipment have dropped considerably over the past several years.[213] In 1968, a brokerage firm on Wall Street adopted fingerprint identification as the method of gaining access to the vault where the stock

208. Parra Interview, *supra* note 158; McCloskey Interview, *supra* note 83; Piper Interview, *supra* note 34.

209. Piper Interview, *supra* note 34.

210. *Id.*

211. Perry Interview, *supra* note 173. First Union ran a test mode with three or four check cashing machines using facial geometry as an identifier. *Id.* One of the problems encountered was customers not standing in the range of the camera. *Id.* For the most part, the facial scanning check cashing machines worked fairly well, but not enough to compel First Union to go forward with biometrics. *Id.*

212. *See supra* notes 192-207 and accompanying text.

213. O'Sullivan , *supra* note 5, at 37.

certificates were held.[214] In 1968, this system cost approximately $20,000.[215] In 1997, a similar system cost about $1700.[216] Purdue Employees Federal Credit Union in Indiana uses fingerprint identification in a self-service kiosk, with each kiosk costing about $500.[217] In 1995, fingerprint readers cost about $2000 while today they are about $99.[218] Because the price of biometrics is dropping considerably, biometrics becomes a more feasible as a method of banking.[219] Considering that billions of dollars are spent each year on identity fraud,[220] biometrics holds a promising future. Not only would it prove more cost effective in the long run, but also it would spare customers the emotional anxiety and stress that often accompanies identity fraud.

In 1999, Bank United set up a pilot program to test the implementation of iris scanning in ATM machines.[221] The bank teamed up with IriScan, Inc. and Diebold, Inc., a leading manufacturer of ATMs to create ATMs that used iris scanning for authentication.[222] These machines were nicknamed "EyeTMs."[223] The pilot found that users experienced no more problems with EyeTMs than they did with regular ATMs, and according to Rob

214. *Id.*

215. *Id.*

216. *Id.* Smaller banks, which do not often have the funds to compete with the technology of larger firms, will watch the bigger banks experiment with biometrics. Sean Hao, *Some Community Banks Not Ready to Offer Customers Online Services,* FLORIDA TODAY, July 12, 1999, 1999 WL 18272921. Therefore, despite the falling prices, smaller banks will allow bigger banks to test the new technology. *Id.* If and when it proves successful, feasible, and cost effective, smaller banks will begin to experiment as well. *Id.*

217. *See* O'Sullivan, *supra* note 5, at 33.

218. Pamila Sherrid, *You Can't Forget this Password: Hint: It's Your Face, Iris, or Fingerprint,* U.S. NEWS & WORLD REP., May 17, 1999, at 49; Joyce, *supra* note 2, at 48. The International Biometrics Group estimates the cost of a finger scanners ranging from $100-$150. Leuchter, *supra* note 47. Because of their low cost, they pull in more revenue (34%) than any other biometric method. *Id.* They are most popular for home or office computers because they are smaller than a touchpad on a laptop computer, thus taking up little space. *Id.*

219. Leuchter, *supra* note 47. *But see* Evangelista, *supra* note 178, at B1 (noting that while finger scanners are rather affordable now, iris scans cost a bit more at $4,000 to $20,000 per scanner).

220. Joyce, *supra* note 2, at 48.

221. Ferguson, *supra* note 4, at 16.

222. *Id.*

223. *Id.*

Coben, executive vice president of Bank United, implementation was "relatively easy."[224] Each EyeTM cost approximately $5000, but the bank anticipates this price dropping as early as the coming year.[225]

From a short-term perspective, the cost of using biometrics is dropping because the price of the equipment is falling.[226] However, a more long-term analysis suggests that using biometrics will remain costly unless all the banks adopt the same method. Despite falling equipment prices, incorporating biometric authentication into customers' daily lives may still prove to be costly or may simply not be worth a bank's investment. If only one method was used and an industry standard was adopted, then costs might drop considerably.[227] However, several methods are currently available to banks. Since test pilots are still being run, banks are in a period of anticipation, while they look to other banks to see if biometric use is cost effective. If, for example, one bank used facial scanning and another iris scanning, a customer who banks at the facial-scanning bank can only use his bank's ATM machines because his facial scan is not in the database of the other banks.[228] This problem would be a great inconvenience to customers and could cost the bank business.

C. *Privacy*

Many biometric authentication methods involve collecting very personal, medical information from customers and storing it in a database.[229] The information in a bank's database can be

224. *Id.* There are basic problems that still need to be worked out including, scalability, reliability, and security of the systems themselves. *Id.* Bank United is concerned over whether its current technology has the capability to store many more iris scans. *Id.* Because so many people use ATMs on a daily basis and because iris scans utilize the most memory, this may pose a potential problem. *Id.* Innoventry plans to install 12,000 iris scanning kiosks over the next three years but does not guarantee that these machines will meet the memory needs required. *Id.*

225. *Id.* Despite the falling cost in equipment, banks still remain cautious in embracing biometrics because of the cost. McCloskey Interview, *supra* note 83; Piper Interview, *supra* note 34.

226. Leuchter, *supra* note 47.

227. *See* Parra Interview, *supra* note 158.

228. *Id.*

229. *See infra* notes 206-13 and accompanying text.

shared with the bank's affiliates.[230] For many customers, relinquishing this information to "strangers" can be a bit unnerving. Several federal statutes protect privacy by not allowing companies to share customer information.[231] The Financial Privacy Act of 1978 provides that certain customer financial records may not be disclosed to any Government authority.[232] In general, the Fair Credit Reporting Act allows consumer credit reporting agencies to provide a consumer credit report only in response to a court order, in accordance with the written instructions of the particular consumer, and to a person that the agency believes intends to use the information for a proper purpose.[233] On November 16, 1999, President Clinton signed the Gramm-Leach-Bliley Act (hereinafter GLB), allowing banks to share customer information with their affiliates without the consent of the customer.[234] Under GLB, banks, brokerage firms, and insurance companies affiliated by common ownership are allowed to share customer information.[235] For instance, if a bank has customer profiles, which include the information entered into the biometric database, an insurance company may gain access to medical records indicating that a certain customer is high risk.[236]

230. 15 U.S.C. §6802 (Supp. V 1999). This is where the Gramm-Leach-Bliley Act is codified. *Id.*

231. *See infra* notes 199-01 and accompanying text.

232. 12 U.S.C. §§3401-3422. This act only prohibits the dissemination of reports to a government authority, which affords the customer some protection to their privacy but not total protection. *Id.*

233. 15 U.S.C. § 1681-1681(u). A consumer report includes a written, oral, or other communication on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. 15 U.S.C. §§ 1681a(d), 1681b allows a consumer credit reporting agency to furnish a report to a third party if it reasonably believes that that person intends to use the information in connection with a credit transaction involving the consumer (i.e. an extension of credit), for employment purposes, for insurance involving consumers, for determining the consumer's eligibility for a license or benefit granted by government, as a potential investor, servicer, or current insurer, or for a legitimate business need. 15 U.S.C. §1681b(3)(A)-(E).

234. 15 U.S.C. §6802.

235. *Id.* The Secretary of Treasury and the Federal Trade Commission are to conduct a study which will examine the purpose of sharing confidential information with affiliates and non-affiliates, potential risks to customers, potential benefits to financial institutions, adequacy of current privacy protection laws, opt-in and opt-out approaches, and potential restrictions. *Id.* at § 508(a). A report on this study is due to Congress on or prior to Jan 1, 2002. *Id.*

236. McGuire, *supra* note 3, at 442.

Consequently, there is a strong concern that insurance companies may increase insurance premiums.[237]

However, this invasion of privacy can also benefit customers. Because biometrics involves using a physical human trait, it can be used to detect disease.[238] Through iris and retina scans, doctors can diagnose diseases such as diabetes, high blood pressure, and arteriosclerosis.[239] Intravenous drug abuse and AIDS can be detected in retina scans.[240] An abnormal fingerprint pattern may also be an indication of a disorder known as CIP (chronic, intestinal pseudo-obstruction), a condition which may involve nausea, vomiting, severe pain, weight loss, diarrhea, and constipation.[241] Furthermore, fingerprints may be suggestive of Down's syndrome, Turner's syndrome, and Klinefelter's syndrome and may be helpful in diagnosing breast cancer, leukemia, and rubella.[242] This technology benefits those who do not go to the doctor because they often do not know they have a disease. Since

237. *Id.*

238. Woodward, *supra* note 69, at 115.

239. *Id.* There is much controversy surrounding whether a bank should inform customers if it is found that they have HIV. *See id.* It would be great protection if used in an early detection case. *Id.* However, it is a highly personal disease, which people may not want others such as banks and insurance companies to know. *Id.* Is it the place of the bank to act as doctor? The same controversy arises with drug abuse. *Id.* Should banks contact law enforcement officials? These are just examples of possible problems confronting banks.

240. *Id.*

241. Woodward, *supra* note 69, at 115 n.146 (quoting *Gastroenterology: Fingerprinting GI Disease,* JOHN HOPKINS PHYSICIAN UPDATE, April 1996, at 5).

242. *Id.* at 116. Down's syndrome is "a congenital disorder characterized by moderate to severe mental retardation, a short, flattened skull, and slanting eyes." THE AM. HERITAGE DESK DICTIONARY 303 (1981). Turner's syndrome, also known as Monsomy X, affects women. NEIL CAMPBELL, BIOLOGY 276 (4th ed. 1996). It occurs when the female chromosomes do not separate properly. *Id.* Normally, women have XX chromosomes, but in Turner's syndrome, they have XO, which means they are missing one sex chromosome. *Id.* This is the only situation where a person can survive with one chromosome less than normal. *Id.* That is, instead of having forty-six chromosomes, they have forty-five. *Id.* It occurs in 1/5000 births. *Id.* Often, XO individuals look like females, but their sex organs do not mature at adolescence, and they fail to develop secondary sex characteristics. *Id.* Turner syndrome is characterized by sterility and a short stature. *Id.* Klinefelter's syndrome also occurs when chromosomes do not split properly, but it occurs in men. *Id. at* 275-76. Men usually have the XY chromosome, but in Klinefelter syndrome, men have XXY. *Id.* This occurs in 1/2000 births. *Id.* Men affected by this syndrome have male sex organs, but their testes are abnormally small. *Id.* It is characterized by sterility and may include breast enlargement and other feminine traits. *Id.* at 276.

many people only go for yearly check-ups, detection also benefits those who do visit the doctor regularly. Using biometrics on a daily, weekly, or even monthly basis could aid in early detection. There still remains the concern that once the information is shared, insurance premiums will rise if an insurance company sees a customer as high risk.[243] While the customer does want to avoid costs, it is just as important to safeguard one's life. If a customer is at high risk for a disease and runs the likelihood of exorbitant medical fees, insurance becomes very important. Having more high-risk customers pay higher premiums ensures that there will be money to cover the expenses.

While the GLB does allow banks to share customer information, it is not without limits.[244] Financial institutions can release information to a third party only if the third party is acting on behalf of the bank and if it will keep the information confidential.[245] In addition, banks must disclose their privacy policy to customers.[246] Therefore, customers will know what information is being shared with the bank's affiliates.[247]

The concern that too many people will have access to a customer's private information relies on the belief that an actual picture of the iris or fingerprint is stored in the bank's database.[248] If this were the case, insurance companies may be able to access that information. However, with the new technology, the actual photo is not stored in the computer, but instead the numeric code to which it is converted is stored in the database.[249] It is simply a nonsensical number with nothing tying the data to a customer personally.[250]

---

243. McGuire, *supra* note 3, at 442.

244. 15 U.S.C. §§6802-6809 (Supp. V 1999).

245. *Id.*

246. *Id.* at §503.

247. *See id.*

248. *Finger-Scan and Privacy, at* http://www.finger-scan.com/finger-scan_privacy.htm (last visited Jan. 6, 2001). The actual picture is not stored in the database. *Id.* More so than other states, the United States heavily values and emphasizes citizen rights to privacy, and thus, biometric technology has been embraced more readily abroad. *Id.* In 1997, the order of adoption of biometrics was Australia, followed by South Africa, South America, Europe, and then the U.S. O'Sullivan, *supra* note 5, at 31 (citing John Parselle, managing director of Fingerscan Pty Ltd.).

249. Parra Interview, *supra* note 158; *Finger-Scan and Privacy, supra* note 248.

250. Parra Interview, *supra* note 158; *Analysis: Biometric Identification, Using*

In addition, while many may fear Big Brother tactics, knowing that there is not one centralized government storage area could ease consumer fears.[251] Since there is no main warehouse where all the biometric information is stored, storage is most often on the unit, local server, or a remote server intended for a single application.[252] Because companies would all have their own systems, it would be difficult for perpetrators to crack the codes or decipher the algorithms.[253] In order to obtain customers information, criminals would first have to learn to crack that particular company's system. Even if successful, however, the numbers in the system are nonsensical, forcing the code cracker to figure out how the algorithms were composed.[254] By educating the public, banks and biometrics companies can help alleviate the public's fear on privacy and dispel any misguided assumptions.

D. Fear of Attack

In addition to the technical difficulties mentioned above, biometrics use presents other concerns. For example, critics argue that if fingerprinting is used, people will cut off fingers. "If you require a thumbprint match, then people would worry about whether a robber would cut off their thumb to get into their bank account."[255] Another skeptic echoed this concern when he wrote,

---

Physical Characteristics Such As A Voice Sample Or Handprint To Identify A Person, supra note 17. Dr. Wayman, director of the National Biometric Test Center at San Jose State University, cites a Harvard Law Review article of 1890, which gave the classical definition of privacy as the right to be left alone. *Id.* Based on this definition, he feels the telephone is the biggest threat to privacy. *Id.* He states that he put his own biometric qualifications on their Website. *Id.* Therefore, people can download his hand geometry, fingerprint, face and no one has ever tried to contact him. *Id.* There is no large database that connect those measures to his identity. *Id.*

251. *Finger-Scan and Privacy, supra* note 248.

252. *Id.* A remote server does not store information gathered from fingerprinting, iris scanning, hand geometry and more. *Id.* It would only hold, for example, the information gathered from one method. *Id.*

253. Parra Interview, *supra* note 158; *Finger-Scan and Privacy, supra* note 248.

254. Parra Interview, *supra* note 158.

255. Murray, *supra* note 127, at B3. Pidgeon states that customers would have a fear that attackers would cut off their thumbs to gain access, yet at the same time, he acknowledges that "[e]ven though the technology requires body-temperature thumb, 'you know you'll have customers worrying about that.'" *Id.* This is not a flaw in biometrics but rather an inadequacy in the banks' education of their customers. *Id.*

"Even today, there are plenty of hoodlums who would cheerfully cut off a thumb in order to . . .raid an ATM."[256] One banker expressed these customer safety concerns as well, stating that he believed biometrics methods are likely to lead to an increase in kidnapping-type crimes. [257] For example, a thief may force a customer to go to the machine and take out money rather than bothering to steal the customer's card and PIN. The thief is most likely unaware, however, that many of these methods can detect when a customer is in distress. For instance, fingerpads can tell when a finger is distressed and alert security. In addition, peripheral cameras may aid in preventing kidnapping crimes.[258]

However, the concern that biometrics may increase kidnapping crimes is valid although some fear may be cured by educating the public. Though customers may be educated on how biometrics works, thieves may not bother to take the time to learn about biometrics. As the public becomes more educated, however, there is a distinct possibility deterrence will increase as well. Potential perpetrators may be deterred by word of mouth, through friends, acquaintances, and family, through advertisements, and from published articles on perpetrators who failed. Furthermore, by being able to alert security when there is trouble, customers may be able to help catch the perpetrator before harm is done.[259] The camera now used in ATM machines catch the perpetrators, but only after harm has been done. By

256. David Hoffman, *A Thumbprint I.D. Could Cost Some Thumbs*, BUS. Wk., Apr. 3, 2000, at 5. Hoffman feels that over the past several years there as been an increased tendency towards violence and therefore, we should second guess using fingerprint identification devices. *Id.*

257. Piper Interview, *supra* note 34.

258. Leuchter, *supra* note 47. According to International Biometrics Group, the price of peripheral cameras has dropped significantly to about fifty to seventy-five dollars. *Id.*

259. *See* Hall, *supra* note 13, at 70. In addition to distressed fingers and temperature changes, panic buttons may also help to alert security. *Id.* at 71. Chicago and the Electronic Funds Transfer Associations in Alexandria, Virginia teamed up to study ATM security. *Id.* One of the ideas they considered was having a panic button, located on the machine, that looks like any other button. *Id.* This would send a silent alarm to officials. *Id.* This may work better with pin numbers or passwords, where a customer could just tack on an additional letter, signaling an emergency. *Id.* This would be very discreet and lead perpetrators or kidnappers to be suspicious. *Id.* However, having silent alarms also provides customers with more security as well as alleviation of fear. *Id.*

alerting security immediately, the perpetrators can be caught sooner.

E. Customer reluctance to embrace new technology

The concept of biometrics as a tool to protect the identity and accounts of individuals is promising, and the cost of biometrics is reasonable, but will customers embrace this technology or resist it? Some believe that biometrics will be greeted with reluctance and resistance.[260] One observer remarked, "A lot of people don't like these things like ATMs or voice mail now. And you're going to tell them to stick their eye up against a bank machine? I don't think so." [261] This statement may be true, but it does not mean that the use of biometrics is a bad idea. Remember, the purpose of biometrics is to provide efficient banking and to protect customers. If we were to rely on this argument of customer discomfort, we would not have e-mail, voicemail, ATM machines, Palm Pilots, PCs, and more. Like anything new, it will be approached with apprehension.

Part of the public's concern can be cured through education.[262] Though these systems can provide for their protection, some consumers resist technological advances because they are not familiar with them or because they feel they are too difficult to learn. The problem is not biometrics, but rather education. Banks must educate the public and their customers about the details of biometrics.[263] What is biometrics? Why should

260. Teresa Dixon Murray, *The Wave of the Future? Technology Turns ATMs into Ad-Omated Teller Machines,* STAR LEDGER (Newark, N.J.), June 1, 1999, at 21 (citing Steve Pidgeon of Union Federal Savings Bank). Some banks are looking to use ATMs for on-screen marketing. *Id.* Based on information that the bank knows about customers, their family, and their spending habits, advertisements tailored to individuals will show up on the screen while users are waiting for their request to be processed. *Id.* Union Federal Savings Bank in Indianapolis, Indiana started using ads on their ATMs in 1996. *Id.* In that year, Pidgeon notes that the bank generated about $90,000 from the ads, and it was estimated that with new full-motion video ads, that number could reach $300,000. *Id.*

261. *Id.*

262. *See* Bloom *supra* note 35, at 15. According to Samir Nanavati, a partner at the International Biometrics Group in New York, states, "[i]f a bank tells [customers] that this is a technology they've tested that's safe and secure and that their privacy is being protected, that mitigates 99.9% of their concerns." *Id.* at 15.

263. Parra Interview, *supra* note 158. Parra suggests educating the public about

we use it? What will we have to do? What will it permit us to do? How does it affect us? Banks must share their privacy policy with their customers, but that alone is insufficient.

Many people have heard that biometrics is an invasion of privacy and that they have to give up some very personal information. What they may not understand is that by doing so, they benefit by helping prevent the fraud that plagues society on a daily basis and preventing themselves from being the victims of identity fraud. Banks share a give and take relationship with their customers. One of the best ways to protect customers is to make customer authentication individualized, thus leaving little room for error. Therefore, customers must give some personal information to the bank in order to assure the best possible protection. Unlike scam artists who "invade" in order to defraud, the banks "invade" in order to protect; .

VI. SOLUTIONS

Much of the public's concern stems from their fear that customer privacy is being invaded. Customers do not like the thought of something as personal as medical information being shared and distributed with the bank's affiliates.[264] There are a couple of solutions to this privacy issue.[265] The first is to store the data in a card, known as a Smartcard.[266] For example, the iris is scanned and converted into a digital code which is stored in a bar code strip on the back of a card.[267] This would be used to verify the user as the one who is actually authorized to use it.[268] Because the

privacy and biometrics through campaigns, classes, and mailings explaining to customers how biometrics benefits them. *Id.*

264. *See supra* notes 206-11 and accompanying text.

265. *See infra* notes 234-48 and accompanying text.

266. Lauren Bielski, *Smart Cards, Coming Up To Bat,* A.B.A. BANKING J., 57 (Nov. 1998). Smartcards can hold biometric information about a customer on them and can be used for a multitude of purposes. *Id.* Customers can purchase airline tickets, buy phone time, or even bread. *Id.* The premise of these cards is to make it an all-in-one card, eliminating the need to carry around so many cards. *Id.* Technology companies are beginning to team up with credit card companies in order to further the advancement of Smartcard use. *Id.*

267. *Id.* While customers lose the convenience of not carrying a card around, they do have the convenience of carrying fewer cards. *Id.*

268. McGuire, *supra* note 3, at 473.

information is stored on the card, the data is not stored in the database, where it may be subject to computer hackers or where it may be distributed to other organizations.[269] Storing the information on a card also eliminates the need for large memory capabilities.[270] While the card can be stolen, thieves cannot gain access to the account. Unlike a pin number, which can be observed over the shoulder, a physical trait is unique to the individual and cannot be replicated by observation.[271]

One banker suggests using the combination of cards and biometrics.[272] While customers lose the convenience of not carrying around a card, using biometrics in conjunction with a card serves the best protection.[273] For example, if a bank is using fingerprinting, a customer's fingerprint is converted into a numeric algorithm that is stored on the strip on the back of the card.[274] When a customer wants to retrieve money from his account at an ATM, he inserts his card into the slot.[275] The card sticks out a little bit. Then, once the strip is recognized in the system, the customer places his finger on the fingerprint reader that is built into the card.[276] The reader is located on the part of the card that sticks out of the slot.[277] If there is a match between the fingerprint stored in the card and the currently read fingerprint, the customer gains access. By using the Smartcard and biometrics together, a stranger cannot gain access to a customer's account even though he or she may hold the customer's card. Also, if someone attacks the card physically, trying to decipher the algorithmic code, the data is automatically destroyed.[278]

---

269. *Id.*

270. *Id.* at 474.

271. *Id.* at 473-74. However, having so much personal information stored in one little card, that is susceptible to theft and loss, may be discomforting to some. *Id.* The idea and the psychological anxiety of knowing that so much personal information is floating around out there and that a stranger may have that card is too much for some to handle. *Id.* In addition, these cards do not lend themselves to the advantage of convenience because customers still have to carry a card around. *Id.*

272. Parra Interview, *supra* note 158.

273. *Id.*

274. *Id.*

275. *Id.*

276. *Id.*

277. Parra Interview, *supra* note 158.

278. *Id.* Parra suggests that Smartcards could further protect us if ambulances

The second solution to privacy concerns would be to allow banking customers the opportunity to "opt-out" of having their personal financial and medical information shared with banking affiliates.[279] Currently, the GLB allows customer to opt out of having their personal financial information shared with third parties, but not with the bank's affiliates.[280] This broader "opt-out" provision may ease the minds of biometrics skeptics. Or, it has also been suggested that there be an opt-in provision, requiring customers to give the banks permission to disseminate personal information and data.[281] "Opt-in" provisions perpetuate better-educated customers.[282] "Opt-out" provisions suggest the need to "get out" of something. Opt "in," however, suggests that this option may be something in which customers may wish to partake. Therefore, they find out more about the situation and then make an educated decision.[283] California and Massachusetts have been considering passing legislation that requires biometrics to be used solely as identifiers which would prevent data from being sold or transferred to third parties.[284] This, however, may lead to the case of fifty states having fifty different laws. Furthermore, the GLB permits states to override privacy provisions if the state laws provide greater consumer protection than the federal protections.[285] Therefore, federal legislation needs to better support the protection of customer financial and medical information before customers are comfortable with the high-tech biometrics industry.

In order for these solutions to be effective, banks must work together to establish an acceptable and successful industry wide standard. One of the greatest benefits of biometric authentication is convenience. If customers are not able to use the closest ATM, their benefit is being infringed upon.

---

were equipped with systems that could read the information on the strip of the Smartcard. *Id.* This way, they can assess the patient's medical information quickly and better tend to the patient. *Id.*

279. McGuire, *supra* note 3, at 474-78.

280. 15 U.S.C. §6802 (Supp. V 1999).

281. McGuire, *supra* note 3, at 478.

282. *Id.*

283. *Id.*

284. *Id.* at 468 n.153 (citing S.B. 71, 1999-00 Cal Leg., Reg. Sess. (1999). *See also* H.B. 4483, 181st Gen. Ct., 1999 Reg. Sess. (Mass. 1999).

285. 15 U.S.C. §6807 (Supp. V 1999).

VII. CONCLUSION

There are several warranted concerns about biometrics. These concerns, however, are not reason enough to compel banks to dispel the idea of using biometrics in ATMs altogether. Reluctance can be cured by education. Uniformity can be cured by communication among banks. Privacy concerns can be cured by federal legislation. The bottom line is that with regards to trust and faith in the banking system, the ultimate goal for customer satisfaction is protection. Customers should feel safe and secure when they are banking. This security can be achieved by using biometric authentication. The concept itself is promising. The means surrounding the implementation of such advanced technology needs to be further studied. However, the concept of biometrics has great potential in our high tech future.

ROBYN MOO-YOUNG