THE INTERNATIONAL JOURNAL OF BUSINESS & MANAGEMENT

Biometrics to Deter Education Related Financial Aid Fraud: 2017 and 2019 Survey Results Reveal Strong Opinions Supporting the Use of Biometrics and Against Using Biometrics

Dahli Gray
Professor, Keiser University, Florida, US State
John Tahlier
Accounting Analyst, Verizon Communications, Inc

Abstract
Education related financial aid fraud is significant. It has not been successfully deterred by prior and existing methods. This article reports survey results exploring using biometrics (e.g., finger prints, eye irises, facial and/or voice recognition) as a method to deter financial aid fraud. It includes and builds on the work of Gray and Tahlier (2018). In 2017, Gray and Tahlier surveyed college graduates under the assumption that they were more likely to have had experience with and/or have awareness of financial aid for education. In 2019 for this article, college graduates were invited to complete the same survey to check for changes in experience with and feeling about biometrics. Strong opinions for and against using biometrics to deter fraud were reported. While the majority of the respondents supported the use of biometrics, the respondents who opposed the use of biometrics were adamantly against biometrics with invasion of privacy as the top concern. Those who support it felt it was the wave of the future and a positive trend. A little over 61% felt that using biometrics to deter financial aid fraud in both 2017 and 2019. Despite using biometrics increased for personal identify protection on iPhones and computers, the opinions about whether using biometrics for protecting against financial aid stayed the same.

Keywords: *biometrics, forensic accounting, forensic auditing, privacy, fraud, financial aid*

1. Introduction

This article reviews that magnitude of financial aid fraud. It discusses the move toward biometrics to protect identity. This article includes and expands on the work of Gray and Tahlier (2018) that was based a survey administered in 2017. For this article, the survey was administered again in 2019 and revealed both strong support for and opposition to the use of biometrics to deter fraud. The use of biometrics identity protection for iPhones and computers increases significantly from 2017 to 2019.

2. Financial Aid Fraud

The United States (US) Department of Education (US DOE) (2016) stated that they "seek not only to protect Federal student aid funds from waste, fraud, and abuse, but also to protect the interests of the next generation of our nation's leaders—America's students" (p. 13). The US DOE also reported a "continuing commitment to promoting accountability, efficiency, and effectiveness" (US DOE, 2016, p. 1, Message to Congress). The US DOE (2015) audits revealed that organizations such as the Higher Learning Commission "did not establish a system of internal control that provided reasonable assurance" (p. 1). The US DOE (2016) "disburses about $150 billion in student aid annually and manages an outstanding loan portfolio of $1.2 trillion … [making this] one of the largest financial institutions in the country" (p. 13). The US DOE reports example after example of a lack of protection from waste, fraud, and abuse (US DOE, 2015; US DOE, 2016). The US DOE (2018) reported the following on page 7:

> The former director of HDS Trucking Institute pled guilty to fraud charges and agreed to pay more than $1.2 million in restitution. The former director used his position to implement various schemes to fraudulently obtain more than $900,000. Among these schemes, the former director deposited HDS students' financial aid refund balances to bank accounts he controlled and caused the school to pay fictitious financial obligations he created and deposited the payments into bank accounts he controlled. …
>
> In our last Semiannual Report to Congress, we noted that a former financial aid director at Columbia University's Teachers College and four students were charged for their roles in a bribery and kickback scam that targeted more than $1.4 million in stipends, scholarships, and student loans. From 2008 through 2017, the former director allegedly approved excessive cost of attendance figures for the students that did not comport with their actual needs or costs of

> living, which increased the amount of financial aid the students were eligible to receive. She also allegedly approved stipends for the students, creating fraudulent request forms for financial awards, which gave the appearance that professors or other school administrators had requested the stipends for the students. When the students received the money, they allegedly kicked back hundreds of thousands of dollars to the former director. During this reporting period, two of the four students pled guilty to their roles in the scam and agreed to forfeit their portion of the proceeds. One student agreed to forfeit more than $620,000, and the second student agreed to forfeit more than $166,100.

The US DOE (2018) reported the following on page 8:

> A former assistant director in the financial aid office of Trident Technical College was indicted for allegedly using her position to override financial aid holds on accounts of students who had failed to meet satisfactory academic progress requirements required for participation in the Federal student aid programs. According to the indictment, the former official recruited people to act as "straw students" for the sole purpose of stealing student aid. After initially attending some classes, the straw students allegedly stopped participating and thus began receiving financial aid warnings as they were not meeting satisfactory academic progress—standards required for continuing to receive Federal student aid. In such cases, a school's financial aid office places the student's account on hold as the student may become ineligible to receive further aid. The former official allegedly used her position and access to the school's financial aid files and removed the holds, resulting in the disbursement of more than $60,000 in student aid to the straw students. Once the straw students received the aid, they allegedly kicked back a portion to the assistant director. ...
>
> A former financial aid official at Delgado Community College pled guilty to solicitation and receipt of bribes. While employed at the school, the former official was responsible for importing and exporting financial aid files as well as the verification of student financial aid applications. In this position, he had access to all financial aid systems and had the ability to manually authorize, award, and disburse aid to students.

While the US DOE 2018 report revealed that financial aid fraud was still a problem, there was no specific mention of it in the US DOE 2019 report. However, fraud at universities was documented to continue. For example, the US DOE (2019) reported the following on page 51:

> The University of Texas Health Science Center at Houston (UTHSCH) entered into a False Claims Act (FCA) settlement agreement, wherein UTHSCH agreed to pay $2.3 million to resolve allegations of grant fraud. UTHSCH was a recipient of National Institutes of Health (NIH) Federal research funding. The United States contends that, from September 1, 2012, to December 31, 2017, UTHSCH misappropriated funds in the amount of more than $1.1 million from the grant.

The need for auditors (e.g., Certified Fraud Examiners (CFE)), strong internal accounting leaders (e.g., Certified Management Accountants (CMA)) and strong external review (e.g., by Certified Public Accountants (CPA)) is clear.

3. Biometrics in the 21st Century

Touch identification (ID) technology such as used by the iPhone and iPad has made the use of biometric ID an everyday reality for many. The advertisements for touch ID illustrate

purchases and protection of assets using a thumb and/or fingerprint. Biometric ID is no longer new and different. Apple "Touch ID ... uses highly sophisticated algorithms to recognize and securely match" finger prints (Apple, 2016). New and different can cause fear or hesitancy.

Common usage indicating both efficiency and effectiveness with enhanced security makes biometric ID not a wave of the future as it is a current methodology. Biometric ID is part of everyday life for those younger than the Baby Boomer generation and for of much of the Baby Boomer generation. For additional security, a combination of a thumb and/or fingerprints plus a numeric passcode can be required. For financial aid applications, the numeric passcode could be the person's Social Security number as it is already a requirement. The thumb and/or fingerprints can add increased protection against fraud.

Biometric ID is one of the most fascinating technologies to emerge in the last several years. The evolution and potential of biometric ID is interesting as well. Most people think of biometrics from only a security standpoint. This may be its main purpose at the moment, but there is so much more application potential for such technology.

Advances in technology and computing power have reduced production costs. These reductions alongside increasing economies of scale, consumer demand, and incidences of fraud have helped to accelerate biometric ID development. The advances of biometrics will continue to expand and be in demand to deter and fight fraud and terrorism.

Application is already used the medical field. An example of this would be the development and application of advanced medical diagnostic equipment, and gene specific treatment of diseases.

4. Ethical Concerns

This technology comes with concerns. One such concern is the issue of privacy (Alterman, 2003). The main issue as it relates to its application for Financial Aid is the collection of a person's biometric ID without their consent or cooperation (Alterman, 2003).

Many who oppose the use of biometrics believe that a person could be singled out by the government, hackers, or associates. These individuals are concerned that ID data (e.g., fingerprints) will be manipulated for revenge (e.g., to frame them, or to discredit them) (Alterman, 2003). Another concern of biometrics from a financial standpoint is that corporations that employ biometric scanners will sell this information to marketers. Marketers might use it to implement target specific advertisements. Another common concern comes from the medical field and is related to the datafield. The concern is that with advances in biometrics a person's medical information might be used to discriminate against them. The concern here is that if a person's medical information is connected to his or her biometric ID, then other people might be able to steal fingerprints and have access to medical records (Laas-Mikko & Sutrop, 2012).
Another way to help protect financial aid and other assets could be the use of cryptocurrency as discussed next.

5. Cryptocurrency

Cryptocurrency is a digital or virtual currency that is cryptographically secured via mathematical computer-based algorithms (Vora, 2015). The difference between cryptocurrency cryptography and current forms of encryptions is the use of a permanent or consistent key (Shahriar, Klintic, Clincy, 2015).
Encryption gets strength from the complexity of characters to a consistent code. Since the code is so complex and long it requires a key which remains constant. This constant key means that anyone with enough time and computing power can figure out the key to access the code to get into the bank or credit card information (Simser, 2013).

Cryptocurrency technology produces an encryption that is constantly changing. A key is created and used for each transaction. This can be seen with such features as Apple Pay, Android Pay, and chipped credit and debit cards. This technology began without online gaming (Vora, 2015).

Online gaming established the use of real currency being used to purchase digital currency. This currency is strictly peer to peer and not in itself subject to governmental or economical market fluctuation in value (Vora, 2015). Out of the online gaming community emerged Bitcoins. Governments are still allowed to dictate individual exchange rates cryptocurrencies such as Bitcoin. This therefore allows the user to use "real" money to buy digital money (Vora, 2015).

The virtual money is then used to buy and sell both digital goods and services or tangible goods and services (e.g., Farmville and Overstock.com). The use of such digital currency started from the online gaming community and has gain worldwide recognition since the emergence of Bitcoin in 2009 (Vora, 2015). This type of technology is one that can greatly influence the f u t u r e of online banking and e-payments.

While this particular technology is not the source of online bank fraud, it is a possible solution to it. The use of cryptography could be used to help fight Financial Aid Fraud through the creation of Financial Aid cryptocurrency. Such a currency could be created by the US DOE.

6. Cryptocurrency to fight financial aid fraud

In this scenario, the US DOE would establish a web or cloud-based application that would create a single use password every time. The students would create an ID that would be based on their finger or palm print. This would then link to any information entered to this finger or palm print.

Then when another person enters the same information, but a different finger or palm print, the system automatically flags it for review. This flag is sent to the school or university that both individuals are applying the fund. The school then would require additional information to be verified (e.g., passport or prior year's tax return information/last reported payroll taxes).

In addition to this, the US DOE would also review the information provided by the students that was initially flagged. Once the school retrieves the necessary information (or the student provides it to the US DOE), it is transmitted to the US DOE for further review. From here the US DOE would compare the additional information that is supplied and compare it to the previous information.

All of which is done by an artificial neural network (ANN), cloud computer, or Internet of Things (IoT) computer system. This system would connect the US DOE with all other government databases (e.g., Federal Bureau of Investigation, Social Security, Internal Revenue Service). The ANN, cloud computer, or IoT computer would process this information and provide the US DOE with a probability result as to who is telling the truth about their identity. Sanger (2015) reported that "clearly the uses are growing as biometrics are used more frequently to assure identity, in secure government facilities and even on personal iPhones."

Continuing on the concerns raised by biometric ID is that once schools, businesses, the government, and current/future employers could share interconnected biometric databases a person's potential will be quantifiable (Rebera, Bonfanti, & Venier, 2014). An example of this would be an employer accessing your medical records via an interconnected biometric
database. The employer then decides to not hire you because you have the gene for breast cancer (Rebera, Bonfanti, & Venier, 2014).

Another example would be a person's biometric analysis identifying a baby's intellectual potential. The child is then socially identified and defined by what he or she may or may not be able to do (Alterman, 2013). Research being

conducted on gene therapy and the human genome project have identified several genes which are predictive of intellectual potential; while others are common in serial killers.

Nations and the global society must seriously consider the ethical concerns. In terms of financial aid fraud, biometric technology may in fact be able to be eliminated altogether. With the use of bimodal biometric ID, it could require that both a finger print and a voice authorization be used, or a palm scan and a retinal scan, or any of the aforementioned items plus a password in order to process a person's financial aid application.

Fleishman (2016) reported that Touch ID now "rules are in place ostensibly to prevent compelling or coercing someone to provide a fingerprint, raising the bar to demanding or cracking a passcode instead." It could be used Touch ID for technology (e.g., iPhone, iPad, computers) and other applications (e.g., student financial aid applications, mortgage loan applications, credit card applications) plus medical record access via Touch ID.

The information provided so far in this article motivated the survey that was administered in 2017 and then again in 2019. The survey results are presented next.

7. Survey Results

The survey respondent demographic information is presented first. The survey questions and summary of the responses are presented next. Examples of respondents' comments (which were not required, but encouraged) are presented followed by conclusions and a summary Survey Respondents' Demographics

Using Survey Monkey, 1,194 college graduates were invited to complete the survey under the assumption that they might have a greater awareness of the financial aid application and distribution processing 2017. The same assumption motivated administering the survey again in 2019, but to 210 college graduates.

Table 1 reports the following regarding the respondents in 2017, none of the respondents were under the age of 18, 15.9% were between the ages of 18 to 29. Twenty-nine-point three percent (i.e., 29.3%) were between the ages of 30 and 44 with 27.9% between the ages of 45 and 59. Respondents who were 60 years old or older represented 26.8% of the individuals who responded to the survey. Table 1 reports the following regarding the respondents in 2019, none of the respondents were under the age of 18, 30% were between the ages of 18 to 29. Twenty five percent (i.e., 25%) were between the ages of 30 and 44 with 29.5% between the ages of 45 and 59. Respondents who were 60 years old or older represented 15.5% of the individuals who responded to the survey.

Table 2 reports that 52.4% of the respondents were female and 47.6% were male in 2017. In 2019, 51.5% were female and 48.5% were male. Table 3 reported for 2017 that the respondents with a household income less than $50,000 were 23.3%. Between $50,000 to $99,999 were 31.7% of the respondents. Those earning $100,000 or more were 45% of the respondents. For 2019, 27% were less than $50,000. For income between $50,000 and $99,000 it was 36%. Those earning over $100,000 were 23.5% of the respondents. Table 4 reported that respondents in 2017 and 2019 were fairly evenly living in all regions of the United States.

Overall, the demographics document that a diverse group of individuals completed the survey.

What is Your Age?		
Options	Response Percent 2017	Response Percent 2019
Under 18	0.0%	0
18 – 29	15.9%	30%
30 – 44	29.3%	25%
45 – 59	27.9%	29.5%
60+	26.8%	15.50%

Table 1: Respondents' Age

What Is Your Gender?	**2017**	**2019**
Answer Options	Response Percent	Response Percent
Female	52.4%	51.50%
Male	47.6%	48.50%

Table 2: Respondents' Gender

How Much Total Combined Money Did All Members Of Your HOUSEHOLD Earn Last Year?	2017	2019
Answer Options	Response Percent	Response Percent
$0 to $9,999	3.4%	3%
$10,000 to $24,999	5.7%	9%
$25,000 to $49,999	14.2%	15%
$50,000 to $74,999	16.5%	22%
$75,000 to $99,999	15.2%	16%
$100,000 to $124,999	13.1%	10%
$125,000 to $149,999	7.1%	4%
$150,000 to $174,999	4.1%	3%
$175,000 to $199,999	2.5%	2.5%
$200,000 and up	6.0%	4%
Prefer not to answer	12.3%	11.5%

Table 3: Respondents' Household Income

United States Region of Residency	2017	2019
Answer Options	Response Percent	Response Percent
New England	7.8%	3%
Middle Atlantic	14.9%	13%
East North Central	16.8%	15.5%
West North Central	8.5%	5%
South Atlantic	15.9%	21%
East South Central	3.8%	4%
West South Central	8.2%	12%
Mountain	7.4%	6.5%
Pacific	16.7%	20%

Table 4: Respondents' United States Region of Residence

8. Survey Questions

Tables 5 summarizes the survey responses for question 1 as to how or whether the respondents had used biometrics. Sixty-seven-point seven percent (i.e., 67.7%) of the respondents had experience using biometrics with only 32.5% having never used biometrics in 2017. In 2019, 87.62% of the respondents had experience using biometrics. This left 12.38% having never experienced biometrics. In 2017, 87 people posted comments regarding question 1. In 2019, 12 respondents posted comments. The comments are summarized next.

In 2017, several commented that they used biometrics to clock in for work (e.g., time keeping, at work to punch in and out). Several experienced the use of biometrics at Disney Parks. Voice recognition was used by financial institutions. Medical and travel (e.g., passport, visa) were mentioned a number of times. In 2019, the comments were similar except no one mentioned Disney Parks.

Table 5 reports that biometrics are used by 44.9% of respondents with their smart phones in 2017 and 74.76% in 2019. Using biometrics relative to background check was reported by 33.1% of the respondents and about the same in 2019. Using biometrics for computer security more than doubled from 2017 to 2019. Online applications and online medical record access more than tripled from 2017 to 2019. Online registration for school doubled from 2017 to 2019.

Which of the Following Have You Used Biometrics (Such As Finger Prints, Facial Recognition, Eye Irises, Vocal Patterns) for Identification? Check All That Apply	2017	2019
Answer Options	**Response Percent**	**Response Percent**
cash a check	12.1%	18.57%
part of a background check	33.1%	33.33%
smart phone	44.9%	74.76%
computer security	15.8%	32.38%
online application (such as job, credit card, loan)	3.8%	10.95%
online medical records access	3.4%	10.48%
online registration for school	1.3%	2.38%
online test taking	3.1%	2.86%
Never used	32.5%	12.38%
Other (please specify)		

Table 5: Biometrics Actually Used

Table 6 reported that in 2017 and 2019 about 61% thought that using biometrics to deter financial aid fraud is a good idea. Twenty three percent thought that it was a bad idea in2017 and 25.36% thought it was a bad idea in 2019. Those checking "Other" in 2017 did not provide comments.

How do you feel about biometrics (such as finger prints, facial recognition, eye irises, vocal patterns) being used as part of the identification process for student applications for financial aid?	2017	2019
Answer Options	**Response Percent**	**Response Percent**
Good idea	61.6%	61.24%
Bad idea	23.0%	25.36%
Other (please specify)	15.5%	13.4%

Table 6: Biometrics for Use to Deter Financial Aid Fraud

Table 7 reports that biometrics should be used throughout the federal student aid process, with 31% checking that biometrics should not be used at all.

Where in The Federal Student Aid Process Should Biometrics (Such As Finger Prints, Facial Recognition, Eye Irises, Vocal Patterns) Be Used: Check All That Apply	2017	2019
Answer Options	Response Percent	Response Percent
throughout (start to finish)	37.4%	38.28%
initial application process	17.9%	25.84%
disbursement of funds to the educational institution	14.2%	12.44%
disbursement of excess funds to the student	19.4%	20.1%
not at all	31.0%	31.1%
Other (please specify)	7.7%	4.78%

Table 7: Where Biometrics Should Be Used In Financial Aid Process

The last part of the survey was an opportunity for respondents to type in comments. It was encouraged, but not required. All of the comments are not included in this article, but are summarized next.

9. Opposed to the use of biometrics

Respondents who felt that the use of biometrics was unnecessary "over kill" versus using due diligence. Many respondents typed something like the following: "This is an unnecessary invasion of privacy. The vast majority of financial aid applications are not fraudulent. It is bad policy to gather this highly private information multitudes of innocent individuals in order to perhaps catch a few cheaters." Several referred to the use of biometrics as creepy and a

move toward the idea of "Big Brother is watching you." Several suggested that chip implantation in humans would be next. One typed the following: "I think it's a slippery slope that could lead to requiring chip implantation and I don't believe financial aid requires that level of security."

Respondents felt that the use of biometrics was a good idea typed something like the following: "I think that there should be proof for voting." Others typed something like the following: "Financial transactions or those that relate to financial or critical functions such as certifications use should biometrics to provide absolute identification fraud or misrepresentation."

Advocates went so far as to type something like the following: "Biometrics should be used for all identification. Social Security Number, date of birth and two-dimensional photos are obsolete." Others typed something like the following: "We are all unique – lets prove it! Cut the fraud out especially in schools."

10. Conclusions and Summary

Biometrics is being used to despite that there is strong opposition to their use. There is also strong support for the use of biometrics. The question still remains as to whether biometrics will be used to deter financial aid fraud. In the meantime, accountants, managers, leaders and forensic auditors have an opportunity to play a significant role to assure the establishment and continuous development of strong internal control systems to assure effective and efficient asset and identity protection. All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

11. References

i. Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. Ethics and Information Technology, 5(3), 139-150. Retrieved from http://pdfsr.com/pdf/a-piece-of- yourself-ethical-issues-in-biometric-identification

ii. Apple. (2016). Touch ID. Advance security. Right at your fingertip. Apple. Retrieved from http://www.apple.com/iphone-6s/technology/?cid=wwa-us-kwbi-iphone&muid=5ADF6211- DADD-44DE-BFBD-

iii. D9930FC1E2DC&mtid=20925d2q39172&aosid=p238&mnid=0v3Wkwpl-dc_mtid_20925d2q39172_pcrid_12358143810_

iv. Gray, D. & Tahlier, J. (2018, January/February). Survey helps begin conversation on using biometrics to deter financial aid fraud. Fraud Magazine (33)1, 54-55.

v. Fleishman, G. (2016, May 18). New Touch ID rules: Why you have to enter your passcode when you wake up. Macworld. Retrieved from http://www.macworld.com/article/3072181/ios/new- touch-id-rules-why-you-have-to-enter-your-passcode-when-you-wake-up.html

vi. Laas-Mikko, K., & Sutrop, M. (2012). How do violations of privacy and moral autonomy threaten the basis of our democracy? Trames: A Journal of the Humanities and Social Sciences, 16(4), 369-381. Retrieved from http://www.kirj.ee/public/trames_pdf/2012/issue_4/trames-2012- 4-369-381.pdf

vii. Rebera, A. P., Bonfanti, M. E., & Venier, S. (2014). Societal and ethical implications of anti- spoofing technologies in biometrics. Science and Engineering Ethics, 20(1), 155-69. doi: http://dx.doi.org/10.1007/s11948-013-9440-9

viii. Sanger, D. E. (2015, September 23). Hackers took fingerprints of 5.6 million U.S. workers, government says. New York Times. Retrieved from http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us- workers-government-says.html?_r=0

ix. Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. Journal of Information Security, 6(3), 206-212. Retrieved from http://file.scirp.org/pdf/JIS_2015063015392117.pdf

x. Simser, J. (2013). Money laundering: Emerging threats and trends. Journal of Money Laundering Control, 16(1), 41-54. doi:http://dx.doi.org/10.1108/13685201311286841

xi. United States Department of Education (US DOE). (2015, November). Semiannual report to Congress No. 71 April 1, 2015 – September 30, 2015. US DOE. Retrieved from http://www2.ed.gov/about/offices/list/oig/semiann/sar71.pdf

xii. US DOE. (2016, May). Semiannual report Congress, No. 72 October 1, 2015 – March 31,2016.

xiii. US DOE. Retrieved from https://www2.ed.gov/about/offices/list/oig/semiann/sar72.pdf

xiv. US DOE. (2018, November). Semiannual report to Congress, No. 77 April 1, 2018 – September 30, 2018. US DOE. Retrieved from https://www.oversight.gov/sites/default/files/oig-sa-reports/archive/17652//sar77.pdf

xv. US DOE. (2019, May). Semiannual report to Congress No. 78 October 1, 2018 – March 31, 2019. US DOE. Retrieved from https://oig.hhs.gov/reports-and-publications/archives/semiannual/2019/2019-spring-sar.pdf

xvi. Vora, G. (2015). Cryptocurrencies: Are disruptive financial innovations here? Modern Economy, 6(7), 816-832. Retrieved from http://www.academia.edu/14244104/Cryptocurrencies_Are_Disruptive_Financial_Innovations_Here