ATHABASCA UNIVERSITY

ANALYSIS OF INSTITUTIONAL LEVEL IDENTITY CONTROL STRATEGIES IN DISTANCE EDUCATION ENVIRONMENT: A SURVEY OF ADMINISTRATIVE STAFF.

BY

ALEXANDER AMIGUD

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF EDUCATION

CENTRE FOR DISTANCE EDUCATION

ATHABASCA, ALBERTA

[MARCH, 2013]

Athabasca University
FACULTY OF GRADUATE STUDIES

Approval of Thesis

The undersigned certify that they have read the thesis entitled

"Analysis of Institutional Level Identity Control Strategies in Distance Education Environment: A Survey of Administrative Staff"

Submitted by

Alexander Amigud

In partial fulfillment of the requirements for the degree of

Master of Education

The examination committee certifies that the thesis
(and the oral examination) is approved.

Supervisor

Dr. Terry Anderson
Athabasca University

Committee members

Dr. Rory McGreal
Athabasca University

Dr. Jeff Zabudsky
Sheridan College

March 26, 2013

Acknowledgements

I wish to express my most sincere gratitude to Dr. Terry Anderson and Dr. Rory McGreal for their guidance and support throughout my first research project. I would like to thank Dr. Jeff Zabudsky for serving on my thesis committee. I cannot thank enough the participants for providing their time and expertise in helping me to complete the data collection component of the research. Without your openness and cooperation this research would not have come to life.

Abstract

Physical separation of students and instructors creates the gap of anonymity. The ability of academic institutions to authenticate students and their academic work at various points during a course is necessary for preserving not only the perceived credibility but also for public safety. This study examines the question of what measures universities with large distance education programs employ to align identity of learners with the academic work they do, as well as examines effectiveness, challenges and barriers to their implementation. The research is undertaken using a multiple case approach and analyzes survey data collected from academic administrators at five officially accredited post secondary institutions in three countries. They are: Athabasca University, Open University UK, Penn State University World Campus, University of Maryland University College and eConcordia– Concordia University's distance learning facility. This study is not an exhaustive attempt to examine all aspect of academic integrity, but rather to create awareness about various learner authentication strategies and also outline challenges and advantages that these measure entail. This study confirms that secure learner authentication in distance education environment is possible. A combination of technology and administrative procedures may facilitate a secure testing environment. Furthermore, with greater pressure to enhance security of learner authentication, the openness of open learning is challenged and may change as we know it.

Table of Contents

List of Tables

List of Figures

CHAPTER I – INTRODUCTION

Background

The integration of technology into learning and teaching has been shown to positively impact achievement, motivation and learning outcomes. Technology improves learning and teaching by making it more effective and efficient, by increasing accessibility to a wider range of learning resources and by creating authentic learner environments that address individual learning styles (Bates & Poole, 2003). However as technology becomes more embedded into the academic structure, it may generate new ethical challenges (Mitchell, 2009). Technological advancements that shape distance learning, teaching, student and faculty support, research and administrative services may create new issues that may not only affect immediate stakeholders, such as learners and instructors, but social structures in general. One crucial ethical concern strongly influenced by the advancement of technology coupled with the growth of popularity of online learning, is academic integrity (Chiesl, 2007; Mott, 2010; Pina, 2010). The ability of academic institutions to verify learner identity during examination and testing is necessary for preserving not only the perceived credibility but also for public safety. With the growing scope of distance education programs that permeate critical areas such as healthcare, airspace, water management and food solutions, universities have a moral obligation to employ secure measures to verify learning outcomes. Smith and Ragan (2005) note that in an educational environment, there typically are two reasons for assessing learners' achievement; the first, is to determine a level of competency and the second is to compare or rank learners' abilities. Moore and Kearsley (1996) maintain that:

> Examination and testing in a distance education setting present some special challenges with respect to security. If students take an exam or quiz at home or at a learning center with no supervision, it is not possible to guarantee the integrity of the test. Consequently, in most distance education programs, students must complete their main exams in a

> proctored setting at a learning center or school… However, the availability of inline testing does not solve the dilemma of ensuring test security. There is still no way to authenticate the learner, although use of desktop cameras… does offer the possibility of actually seeing the candidate to confirm their identity (matched against photo ID). (p. 155)

However, as it will be discussed further, a number of educational technology companies are introducing sophisticated surveillance claims that may challenge Moore and Kearsley's claim of 'not possible' that was made in 1996. The issue of identity control or lack thereof is particularly prominent in the case of diploma mills. A diploma mill is defined by Pina (2010) as an institution that provides credits for "unverified life experience" (p. 124). He notes that credibility of distance education is affected by questionable practices of the diploma mills, and argues that many of the negative issues in distance education arise as a result of "difficulty distinguishing between what occurs in legitimate distance education and what is done by diploma mills" (p.121). However, legitimate academic institutions are not immune to academic misconduct including identity fraud. Weak identity control measures are not uncommon among legitimate academic institutions and put them at risk of being perceived as less credible.

Credibility entails due diligence. The officially accredited universities have a commitment, moral and legal requirements to align students' achievements with their identities. These institutions issue degrees only to those who demonstrate competence and academic accomplishment, whereas the diploma mills issue diplomas to anyone who is willing to pay a service fee. In one case, Trinity Southern University, the Texas diploma mill awarded an MBA degree to a cat (School that gave MBA to cat sued, 2005). Dog owners that have strong emotional ties with their pets have an equal opportunity to invest in their pets' educational credentials. According to Wikipedia (n.d.) there are fourteen known cases of animals (eight cats and six dogs) with fraudulent diplomas or certificates. Therefore, institutions' ability to align students' competence with identity is one of the fundamental features that distinguishes legitimate schools from the diploma mills.

About the Researcher

I am a graduate student in the Master of Education in Distance Education program at Athabasca University. My primary research interest is educational technology. This study is motivated by a gap in the research literature that compares the effectiveness of identity control methods for authentication of student work. This subject is very close to my heart because I work as an Information Technology (IT) and Special Projects manager, facilitating corporate training programs, developing software and supporting staff at over twenty remote offices.

Purpose

The study examines the cases of five leading post secondary institutions offering distance education in three countries. They are: Athabasca University, Open University UK, Penn State World Campus, eConcordia– Concordia University's distance learning facility and University of Maryland University College. The study provides an analysis of the identity control strategies employed by the five universities, discusses challenges with the existing identity control measures and examines the barriers to their implementation from the perspective of university administrative staff. This study calls for a new organizational strategy to address academic misconduct and identity control measures that minimize opportunities for identity fraud in an online environment. This study is not an exhaustive attempt to examine all aspects of academic integrity, but rather to create awareness about various learner authentication strategies and also, outline challenges and advantages that these measures entail.

Research Questions

The primary research question explored in this study is:

What measures do universities with strong distance education programming employ to align identity of learners with the academic work learners do? If there are no identity control measures employed what are the barriers to implementation ?

The subsidiary research questions explored in this study were:

1. How effective are these control measures?
2. What are the challenges associated with identity control measures already implemented, if any?
3. Are there best practices emerging for authenticating the identity of remote learners?

Statement of the Delimitations

1. This study is limited to the examination of institutional level learner authentication strategies.
2. The sample is limited to five institutions, where three universities are distance education institutions: Athabasca University, Open University UK, University of Maryland University College and two are distance education extension facilities of traditional universities: Penn State University World Campus and eConcordia– Concordia University's distance learning facility.
3. Data collection was limited to electronic questionnaires, email, structured interviews through telephone and review of documents that address learner identity control issues. Only documents made readily available by the respective institutions were examined.
4. Strategic convenience sampling was employed to select one administrative staff member from each university to create a total group of five participants, to answer a brief questionnaire and participate in a follow up interview or provide additional information by email.

Definitions

Academic Identity Fraud is a form of cheating that involves deliberate impersonation of another individual in person or through the use of communication technology. Mott (2010) notes that one of the drawbacks of assessment methods that do not require identity verification is a potential for attracting proxy test takers.

Academic Integrity is a set of values that guide the academic community. These include the values of honesty, avoidance of misrepresentation, trust and

fairness. The avoidance of cheating and plagiarism is the fundamental requirement of academic integrity.

Academic Integrity Policy is a document that provides members of the University community general notice of appropriate academic behaviors and identifies prohibited behavior and academic conduct. Academic Integrity Policy may vary from institution to institution and include bylaws and local regulations.

Academic Misconduct is the umbrella term used to describe activities that violate an academic integrity policy. "This may include issues such as copying work from another student with or without their permission, cheating during exams, copying text from books or journals and passing it off as one's own, falsifying or inventing laboratory data or getting another person to write an essay" (Sheridan, Alany & Brake, 2005, p. 241).

Authentication is a process of validating one's identity. Bailie & Jortberg (2008) highlight the "four main premises of identity validation:

1. Who we are—fingerprints, iris scans, voice recognition, DNA, and so on
2. What we have—birth certificate, driver's license, passport, digital tokens, and so on
3. What we know—in-wallet and out-of-wallet information about our past, such as financial, geographical, and demographic data
4. Where we are at a specific moment in time—[face-to-face or] video monitoring, IP address, telephone access, and so on" (p. 66).

Authorship is a process in which an individual originated or created an original piece of work.

Cheating is dishonest academic behavior driven by a self-benefit motive. The term encompasses a large group of unethical behavior such as plagiarism, identity fraud, fabrication and falsification of data, ghost writing, collusion, proxy test taking, etc.

Collusion is a form of cheating, where one's academic work is produced as a result of collaboration with one or more individuals without proper permission, attribution or authorization.

Distance Education is a method of teaching and learning in which the learner is separated from the instructor by space or time and both depend on the use of communication technology to bridge that gap. For the purposes of this study, only web-based courses will be considered. Therefore, computer communication technology is responsible for the delivery of information and interaction through space or time.

Distance Learning is a process that encompasses a broad range of activities and development of learners enrolled in a distance education course of studies.

Diploma Mill is an organization that awards academic degrees with no or substandard academic study and/or without proper accreditation from government authority to award degrees and/or verification of student identity. Pina (2010) notes that "providing credits for unverified life experience is a hallmark of diploma mills" (p. 124).

Ghost Writing is a form of collusion often offered as a service, where written works of one author are credited to another author in exchange for a fee.

Identification is a process of establishing one's identity. Bailie and Jortberg (2008) note that:

> In its truest sense, this is an assurance that an individual presenting himself as Bill Jones actually is Bill Jones… Identification activities begin with the collection of personal information used as further proof of identity, including facets such as legal name and address, social security number, academic records, and so on. Subsequent to formal enrollment, online students are issued a token (such as a user name) to be used as an identifier to access a secured online course. (p.66)

Learning Management System (LMS) is a software application suite for the administration and delivery of web based courses.

Multibiometrics is a process of using multiple biometric sources for validation of one's identity.

Online Education *see Distance Learning.*

Plagiarism is a form of cheating, where one's academic work includes inappropriate expropriation of intellectual property of others without providing a proper acknowledgement.

Proxy Test Taking is a form of identity fraud where one individual agrees to impersonate another individual to complete a part of academic work.

Software Only Biometrics computer software that analyzes anatomical, physiological, or behavioral characteristics of individuals to confirm their identity.

Spyware is a software application that covertly collects and transmits information.

Turnitin is an online plagiarism-detection tool designed to help educational institutions and students identify plagiarism or improper citation of references in written assignments (Sheridan et al., 2005).

CHAPTER II - REVIEW OF THE LITERATURE

This review highlights articles, studies and research literature that overview the main challenges and potential solutions to student authentication in a distance education environment. These include a look at the magnitude of the problem, variations of the academic integrity issues and motivations of those who violate academic integrity. It discusses the technological initiatives undertaken by universities to ensure proper authentication of the student work. A significant portion of the review examines the remote authentication technologies such as biometric authentication and remote proctoring. Several previous pilot studies that evaluated the users' perception and acceptance of these technologies are discussed in detail.

Much literature on academic misconduct in distance education is concerned with prevention of plagiarism, with wrongful appropriation of intellectual property and with the technological means of prevention. There is little research done on the institutional level identity control measures or their effectiveness. Many scholars have noted a problem of academic misconduct that results from unprecedented growth of distance learning and physical separation of learners and instructors (Chiesl, 2007; Grijalva, Nowell & Kerkvliet, 2007; Mott, 2010; Sheridan et al., 2005). In addition, there are many benefits of using online assessments not only in distance courses but in traditional courses as well. These may include cost savings and greater accessibility. Mott (2010) points out that:

> It is important that the distance educator become aware of the opportunities for academic dishonesty that exist in the online delivery environment, understand how to minimize those opportunities, and avail himself or herself of the technology [or practices that are designed] to detect dishonesty when it does in fact occur. Only then will the integrity of the environment reach the level that it must in order for the promise of distance learning to realize its fullest potential. (p. 44)

Magnitude of Academic Integrity

A study conducted by Kennedy, Nowak, Raghuraman, Thomas, and Davis (2000) explores student and faculty perception of cheating in an online environment. One hundred seventy-two students and sixty-nine faculty members from a midsize traditional university participated in the survey. A majority of the students surveyed in this study (109 participants) had previously completed an electronic course and were familiar with distance learning. The findings suggest that "both faculty and students believe it is easier to cheat in distance learning classes" (p. 309).

McCabe and Trevino (1996) examine the magnitude of academic dishonesty and longitudinal trends of student behavior by comparing data from two studies involving multiple campuses and large samples. The authors surveyed "over 6,000 students at 31 campuses around the country, using a sample of schools generally small to modest in size that had highly selective admission policies" during the 1990-91 academic year and published the results in 1993. The study was an approximate replication of " the landmark study Bill Bowers conducted in 1963 involving more than 5,000 students on 99 campuses of all sizes and descriptions…Both studies asked students about academic dishonesty on tests and examinations and on major written assignments. Although the differences in the samples used in these two studies limit direct comparisons, together they do provide an important perspective on student cheating" (pp. 29-30).

The patterns observed in these two different studies almost 30 years apart are relatively consistent and at the same time raise serious concerns about academic integrity. The findings suggest that over 80 percent of students cheated at least once on a major written assignment. The results of McCabe and Trevino (1996) study show that "82 percent of the students surveyed in 1963 admitted to at least one instance of cheating on written assignments compared to 84 percent of the students surveyed in 1993" (p.31). These figures do not include the instances of collusion which is a growing trend that has increased by 38 percent since 1963. McCabe and Trevino (1996) maintain that the number of students who admitted to engaging in collusion "jumped from 11 percent in 1963 to 49 percent in

1993…Indeed, 83 percent of the students surveyed in 1993 did not think collaboration was serious cheating, and almost one in four did not think it was cheating at all" (pp.31-32). The perception of seriousness of academic misconduct varies significantly among students. Academic integrity policies are not viewed as an absolute and only measure of acceptable behavior but only as a guideline. McCabe and Trevino (1996) explain:

> … a minority of the students in the 1993 study view fabricating/falsifying bibliographies (42 percent) and copying material without footnoting (26 percent) as serious cheating. In contrast, a strong majority of these same students do view plagiarism (76 percent) and turning in work done by someone else (80 percent) as serious cheating. (p. 31)

Although, the research by McCabe and Trevino (1996) was aimed at analyzing data from traditional college setting where testing and examinations are proctored, one may argue that the trends identified in the study are transferable to the distance education environment, where project based assessment may replace secure examination and where proctoring is not always an option. A study by Scanlon and Neumann (2002) focuses specifically on the influence of the internet on academic integrity. The study was undertaken to test an assumption that the internet makes plagiarism easier. Authors were seeking to answer the following questions: "What is the incidence of Internet plagiarism among college students? [and] What are students' perceptions of Internet plagiarism by their peers?" (p. 376). An anonymous pencil-and paper survey comprised of 60 Likert-like scale questions was administered to 180 students on 9 campuses of traditional institutions. In addition to questions about the role of the internet in cheating behavior, the participants were asked to estimate the incidence rate of plagiarism conducted by their peers. "Specifically, we wanted to know if any marked disparity exists between self reports of plagiarism and students' perception of what is taking place around them" (Scanlon & Neumann, 2002, p. 378). One of the challenges with academic integrity research is that it heavily relies on self-reporting. The research of Scanlon & Neumann (2002) is even more challenging because the subject of their study is dishonest conduct, they stress that "[i]n

general, self-reports of cheating are high, although estimates vary widely, with 9% to 95% of those asked admitting to some form of academic dishonesty" (p. 375).

The results suggest that acts of conventional plagiarism were similar in frequency to that of online distance education. A minority of students, 19.0% admitted copying and pasting text without proper citation sometimes whereas 9.6% admitted to doing it often or very frequently. Another 5.4% of participants admitted copying an entire paper sometimes and 3.2% often or very frequently. As well, 6.3% admitted to purchasing a paper sometimes, whereas 2.8% of participants admitted to purchasing an off the shelf paper often or very frequently. Online plagiarism reports were similar. Copying text without proper citation was reported by 16.5% of participants that did it sometimes and 8.0% did it often or very frequently. The online paper mills were used by 6.0% students sometimes and 2.3% admitted to purchasing papers often or very frequently.

The perceived incidence of plagiarism performed by peers was reported to be significantly higher than that of indicated in self-reports. Scanlon and Neumann (2002) maintain that while 8.0% of students admitted to copying information from the Internet without proper citation often or very frequently, their estimate of peer plagiarism was at 50.4%. Purchasing papers from online paper mills followed a similar trend, 8.3 % admitted to purchasing papers sometimes to very frequently, they estimated that 62.2% of their peers "patronize those sites at that rate" (p. 380).

Scanlon and Neumann (2002) argue that students who admit engaging in cheating behavior may not limit its scope to only one medium, but rather employ both conventional and internet plagiarism. The internet may simplify access to a wider source of information, but whether or not it influences one's preference for cheating is still unknown. The authors also note that since 24.5% of the students self-reported to engage in online plagiarism, "[the numbers] should be cause for concern, although these numbers do not suggest an epidemic of Internet-facilitated plagiarism" (p. 381).

Diploma Mills

The diploma mills pose a different problem; they issue degrees to anyone willing to pay a service fee. The identity control measures that help to align student identity with academic achievements are intentionally eliminated allowing anyone, and in some cases domesticated animals to receive academic designations (School that gave MBA to cat sued, 2005; Wikipedia, n.d.). Such unethical practices undermine the public perception of credibility of accredited universities that offer distance courses and programs. Pina (2010) examines the issue of credibility of distance education and argues that many of the negative issues in distance education arise as a result of difficulty distinguishing between "what occurs in legitimate distance education and what is done by diploma mills" (p. 121). He notes that lack of consistent academic standards, a confusing and multi-layered system of accreditation, curricular and instructional autonomy affect the perceived credibility of distance education. "Inconsistencies within this system of accreditation make it confusing for the general public and advantageous for those who run diploma mills...Diploma mills constitute a billion-dollar industry that siphons off potential college and university students (particularly during time of economic distress) and damages the reputation of legitimate distance education. One way to combat this threat is for the higher education community to come together in strong support of legitimate distance education" (Pina, 2010, pp. 123-124).

Reasons for Cheating

There are two categories of cheating behavior according to Bunn, Caudill, and Gropper (as cited in Grijalva et al., 2006); the planned cheating and the panic cheating. Grijalva et al. (2006) maintain that:

> Although both types of cheating involve weighing costs and benefits, if social norms differ for planned and panic cheating, the subjective costs and benefits may be different for planned and panic cheating. Planned cheating may involve making crib sheets for tests, copying homework, or plagiarizing a paper; it occurs with full knowledge that it is wrong. Panic

> cheating, on the other hand, occurs during a test when the student finds herself at a loss for an answer. Although she did not plan to cheat, she looks at another student's paper and copies the answer. Being premeditated, planned cheating may be viewed as more dishonest than panic cheating and perceived as having a greater social cost. (p. 184)

This view tallies with that of Sheridan et al. (2005) who argue that students cheat either intentionally or unintentionally. However, the latter is attributed to a lack of understanding of academic policies and standards or due to cultural differences in beliefs about ethical behavior. Thus, student education about academic integrity policies may eliminate unintentional cheating.

These findings tally with that of McCabe and Trevino (1996) that also stress the importance of academic integrity culture that promotes the values of honesty and trust. Their findings suggest that "the most important question to ask concerning academic dishonesty may be how an institution can create an environment where academic dishonesty is socially unacceptable. One of the most discussed strategies for creating such environments is academic honor codes…[and there is] convincing evidence that cheating is generally lower on campuses with such codes" (p. 30). However the socio- cultural influences extend far beyond the campus level and by the time high school graduates become university students they may already be primed with the goal of competitiveness and success, thus taking a shortcut that maximizes personal utility is an acceptable behavior. The mainstream media publicizes and often glorifies acts of questionable ethical conduct that often yields positive outcomes. "[S]tudents are somewhat skeptical when they arrive on campus and hear orientation speeches about the lofty virtues that underlie the educational process" (McCabe & Trevino, 1996, p.29). This notion is congruent with that of Chiesl (2007) who suggests that cheating may be reduced by minimizing competition among students since minimized pressure to succeed eliminates the need for students to use cheating as justification.

Cheating Methods

Technology presents a cornucopia of tools for cheating. Mott (2010) notes that the advances in computer and communications technology lead to the development of "many innovative methods that may be employed by students who wish to cheat on online assessments" (p.33). They vary from unauthorized use of "textbooks and class notes to proxy test takers, who may be easily utilized if some form of identity verification is not employed. It is clear that an instructor is unable to control a student's use of unauthorized sources of information during an assessment where a proctor is not present" (Mott, 2010, p. 33).

Another important concern raised by Sheridan et al. (2005) is the increasing availability of over-the-counter essays and websites that offer professional writing services. The former may be addressed by a plagiarism-detection tool such as Turnitin, which will be discussed in the following sections. However, the latter in the absence of authentication and authorship validation measures is very difficult to detect and prevent as ghost writers tailor assignments according to one's requirements. The two other means of cheating on distance assessments discussed by Mott (2010) are that of the sharing information electronically, via e-mail, text messages or cell phones as well as the use of spyware that covertly monitors other students' computers.

In a survey conducted by Kennedy et al. (2000) one hundred seventy-two students were asked whether the online class offers a better opportunity for cheating, whether they have been previously caught cheating and whether they perceived cheating improves one's exam scores. The findings indicate that there is no correlation between students' perception of the ease of cheating in distance learning classes and previous cheating experience. However, "in all conditions the majority of the students felt it was easier to cheat in distance learning classes" (p.309). In a survey of sixty-nine faculty members, Kennedy et al. (2000) asked what cheating methods distance learning courses encourage. The findings indicate that the main concern of the faculty is with off the shelf papers and completion of assignments by someone other than the student. "The methods currently being used in the regular classroom would continue to be used" (p.309).

Proxy Test Taking

Unlike plagiarism that could have been accidental and performed by a single individual, proxy test taking requires strategic planning and collaborative efforts. Proxy test taking services are not explicitly advertised as they no longer fall under an administrative type of offense, but rather can be prosecuted under the criminal justice code as forgery of official documents is often used to deceive test administrators or proctors. In a traditional school setting, identity documents are verified by proctors, thus to deceive a proctor, a proxy test taker must forge the identity documents. In an online environment where username and password are often the only credentials used for identity verification, there is no need to forge documents. Changing identity is as easy as typing two strings of text on a login screen. Proxy test taking may be sought by those who lack confidence or knowledge to write a test. Potential customers may not only be undergraduates suffering from test anxiety, but as recent media reported, adult professionals.

An article by Branston (2012) published in the Memphis Flyer newspaper in July of 2012 discusses one such case. He reports that a group of teachers and aspiring teachers paid between $1,500 and $3,000 per test to professional test takers that registered in the exam administered by Educational Testing Service using false identification. This large scale proxy test taking ring, according to the United States Attorney General Office, was operating between 1995 and 2010 and involved over 50 proxy test takers. The individuals who contracted the services "believed they were unable to pass PRAXIS examinations" and arranged for a professional test taker to take examinations in lieu of them. "Parts of the test are required to teach specific subjects in some states including Arkansas, Mississippi, and Tennessee" according to Branston (2012), and therefore, this was not an isolated incident but rather a large scale operation. The investigation was prompted by a vigilant test proctor that noticed an individual writing the same test twice in the same day.

In a separate case, Anderson and Applebome (2011) reported that 20 teenagers at five schools were arrested in a case of test taking for Scholastic Aptitude Test (SAT) and American College Testing (ACT), the standardized tests

for college admissions. Felony charges were laid in 5 cases, the remaining 15 individuals faced misdemeanor charges for paying between $500 to $3,600 to test takers who were skilled at crafting fake identification cards that were used for exam registration. This case is significant in that it raises a red flag about test security measures as male test takers were able to register in lieu of female examinees. What is more troubling is that proxy test taking is a service routinely provided to those who have the financial means. “According to prosecutors, principals, parents and teenagers here on Long Island’s Gold Coast, it was common knowledge at some of the nation’s most prestigious high schools that if you had the money, you could find someone with a sharper vocabulary and a surer grasp of geometry to fill in the blanks for you” (Anderson & Applebome, 2011).

In yet another example of proxy test taking, this time the incident occurred in United Kingdom, two individuals were charged and jailed for taking health and safety on behalf of several construction workers. This fraudulent activity was aimed at passing the safety test to obtain skills cards. “They had been caught by staff at CITB-ConstructionSkills’ test centre… and were sentenced to nine months each… and will be deported once they have served their sentences”. The test centre staff “discovered the fraud, known as proxy testing, after realizing the men had taken multiple tests using several other workers’ identification passes which bore their own photographs” (Morby, 2012).

Mobile Devices

Mobile devices play a pivotal role in enabling mobile learning. However, electronic communication and computing devices capable of capturing, retrieving and processing information also pose a challenge for the exam integrity. They may not only simplify finding solutions to a variety of test problems, but also streamline capture and distribution of digitized exam documentation. These devices are compact, easy to conceal and provide a high processing power. These include smart phones, tablets, portable computers, digital multifunction watches and programmable calculators with wireless communication capabilities. Cell

phones and tablets often have built-in digital cameras and audio recorders allowing capture and sharing of high resolution images and videos as well as capable of recording audio signal. Miniature digital recorders and transmitters capable of recording both audio and video signal come in various shapes and sizes and may be disguised as ordinary items such as writing instruments, wristwatches, jewellery and even shirt buttons.

These devices are highly accessible and are generally easy to use. They are available from local spy shops, from home security stores or even from online auction websites. This suggests that test security will always remain a hot topic for students and university administrators. "[M]ost academic institutions are dealing with the problem of electronic devices through the following means: Communication, information and awareness, policies and action by administrators and faculty, and technological solutions… Universities should revisit their honor codes and update them in response to technology" (Faculty Senate Committee on Technology, 2005, pp. 1-2). Communication appears to be the preferred method of instructors and administrators since technology is not yet able to provide adequate policy enforcement tools. "Faculty must address the issue of academic integrity and communicate to students what is expected of them from the standpoint of ethical academic behavior. Faculty can reinforce this by specifically mentioning policies in the syllabus, in lectures, and prior to any exam" (Faculty Senate Committee on Technology, 2005, p. 2).

Academic Misconduct Prevention Strategies

There are several methods available to reduce the amount of student cheating. Kennedy et al. (2000) argue that cheating based on technology must be addressed by technology-based solutions. The position of Sheridan et al. (2005) on prevention of academic dishonesty tallies with that of Kennedy et al. (2000). He maintains that technology has already been employed to address the issues of plagiarism by developing tools such as Turnitin. These computer tools are able to identify the strings of text found in its database and public web pages. Each assignment submitted to Turnitin receives a similarity report. Despite its

effectiveness at detecting multiple use of the same text, and popularity among universities, one may argue that Turnitin is ineffective in identifying original work written by someone else for the student as could be the case with shadow writers. This tool only targets one problem, that is plagiarism among a variety of cheating techniques available to students. Many instances of plagiarism are direct copies from web pages, therefore, a basic way of identifying plagiarism in written text may include running search queries on popular search engines. This strategy may not be as comprehensive as the Turnitin database search, but may prove effective in identifying copies from free online encyclopedias.

According to Chiesl (2007) cheating may be eliminated by administering multiple versions of the same test, having proctors oversee the assessment, and by giving verbal warnings about cheating. However, one should exercise caution relying only on teaching assistants for the provision of proctoring services. Not only the presence of proctors, but also the type of proctors involved in exam administration affect the rate of cheating. Kerkvliet and Sigmund (as cited in Chiesl, 2007) note that "[u]sing tenured or tenure-track faculty tends to reduce cheating. Using only teaching assistants in a classroom will increase the amount of cheating" (p. 205). Chiesl (2007) notes that by minimizing competition among students, cheating will be reduced, as a result of minimized pressure to succeed that forces students to use cheating as justification. He offers a pragmatic method of reduction of cheating by online students. His method is comprised of four practical courses of action. They are: "[1] disseminate information to distant students; [2] change the process used by students to turn in written assignments; [3] change the process by which exams are administered; and [4] create a nonsequential chapter assortment of questions" (p. 205). By allowing multiple test-taking attempts and granting deadline extensions to students, the pressure to take a shortcut in order to succeed at an examination is reduced, as there is a second chance to start over again. Although this suggestion may sound overly generic, a study of Chiesl's (2007) pragmatic method offers promising results. The results of anonymous online survey administered to 149 students indicate that they "were satisfied with the amount of the learning they achieved. Students

appreciated the ability to take each exam multiple times. Most importantly, students reported a lesser incidence of online cheating compared to other Web classes" (p. 210).

In a study conducted by Mott (2010) a statistical analysis is used to identify cases of academic dishonesty by 53 students enrolled in two aviation technology courses at the Indianapolis Campus of Purdue University during the 2009-2010 academic year. The study examined the commonality of incorrect question responses between the datasets. "The process, then, of detection of cheating on concurrent online assessments becomes one of calculating pairwise vectors of identical, incorrect answers between all students taking an exam concurrently, ascertaining the number of identical, incorrect responses per pair, and then fitting the aggregate data to a Pólya distribution" (pp. 35). The findings are promising and offer alternative detection methods to the ones used by a plagiarism detection software. Mott's (2010) suggestions to prevent cheating are remarkably similar to those of Chiesl's (2007). He points out that the best practices applicable to online assessments conducted using a content management system and consisting of multiple-choice questions include: randomizing questions selected from a large pool of questions; allowing only one question to be displayed at a time; creating a large number of exam versions, timed and with a low grade weight; allowing the exam to be taken for an entire week with multiple attempts.

Isa, Samah, and Jusoff (2008) take a non technical approach to prevention of cheating and stress that appeal to reason and reinforcement of values is an effective prevention tool. "The statements of the policy aim to teach students to understand that an electronic community requires people to behave responsibly and use the resources accordingly. For the academics, the policy is to make them aware of their responsibilities and expectations as online instructors and to exhibit legal and ethical behaviours" (p. 455). This view is similar to that of Sheridan et al. (2005). The importance of the honor codes and cultures that condemn cheating is also stressed by McCabe and Trevino (1996).

Bailie and Jortberg (2008) note that assessment of remote learners and identity validation aspect of it in particular, has historically been a challenging issue often cited by critics of distance education. In response to this challenge, institutions have developed several alternatives to traditional testing and examination to address the problem of limited security over remote testing environments. Proctored examinations through examination invigilation networks remain a popular choice of institutions offering distance courses. Institutions have also "increased emphasis on student portfolios, papers, projects, and quizzes [and in some cases opted for] complete avoidance of secure testing" (Bailie & Jortberg, 2008, p. 65). There is also a wide variety of technology based solutions available to institutions ranging from plagiarism detection tools and remote proctoring services to biometric authentication systems that will be discussed in detail in the following sections.

Authentication Technologies

The following sections discuss examples of authentication technologies and highlight the results of some of the pilot projects conducted by universities to address the challenge of remote learner authentication. The pilot project results suggest that biometric and remote monitoring technologies hold a great promise in providing institutional administrators with the means of aligning student identities with the academic work they do. Regardless of technology employed, an identity enrollment needs to be accurately completed prior to the authentication stage. The quality of authentication depends not only on the type of technology used, but also on the quality of initial user identification. Technologies that provide multi- factor authentication add an additional level of identity assurance and therefore, minimize opportunities for identity fraud.

Biometrics

Unlike traditional online user authentication methods that employ verification of information that the user knows, such as a password, student number or the answers to personal questions, biometric authentication systems verify anatomical, physiological, or behavioral characteristics of individuals to

confirm their identity. A biometric key is often used in conjunction with password authentication, adding an extra layer of security. For example, to write an online exam, a student must first login to the LMS or examination portal using a password, followed by authentication through keystroke dynamics using a keyboard or face recognition using a webcam.

Some software and hardware solutions have been developed by the private sector to address challenges of educational institutions. For example, Biometric Signature ID (BSI) develops identity authentication solutions that "reduce identity fraud through its' patented BioSig-ID Online™ biometric handwriting and gesture technologies" (BioSig-ID, n.d.). The technology allows verification of biometric signatures using a personal computer with a pointing device such as a mouse, stylus or touchpad, eliminating a need for additional hardware such as the biometric scanner. According to Levey and Maynard (2011) "biometrics are difficult to duplicate and nearly impossible to share. Because authentication through biometrics can be applied to multiple course elements, assessments are not limited to tests as is the case with proctoring or monitoring (digital proctoring).Additionally, biometric systems have low implementation costs and staffing needs, unlike traditional and digital proctoring" (p.6). Other companies have stepped up to address this problem and offer a combination of biometric authentication and remote proctoring services. Another company, Kryterion Inc. "utilizes remote video monitoring to observe test takers where they live, learn or work" (Kryterion, n.d.). Both solutions have been pilot-tested by post secondary institutions and the results of these initiatives will be discussed in the following sections.

Remote Proctoring

Proctoring remains a popular method of ensuring the integrity of distance learning tests and exams. There are both traditional and computer mediated proctoring solutions available to institutions. The latter often incorporates biometric technology to confirm learner identity as well as remote monitoring technology, while the former requires institutions to establish relationships with

external examination centers. The Canadian Invigilator Network (CIN) is a network of proctoring centers where student examination is monitored by trained proctors. Several universities including Athabasca University and Thompson River University have established strategic alliances with examination centers in Canada and abroad. Students are not required to use the CIN examination centre closest to them and may use any approved examination centre that meets their needs or schedule. Computer mediated proctoring eliminates the need for travel but requires installation of biometric and remote monitoring devices at learners' location. Software Secure Inc. has developed a "Remote Proctor Suite" a digital proctoring solution that is designed to enhance academic integrity of exams taken remotely. The company describes it as "[t]he gold-standard in remote test integrity, Remote Proctor Pro addresses every area of exam security by authenticating his or her identity [using biometric technology] and controlling a student's computer while watching and listening to the exam environment" (Software Secure, n.d.). Similar solutions have been developed by Kryterion Inc., which describes itself as a "full-service test development and delivery company that provides world-class online testing technology" (Kryterion, n.d.). This technology was pilot-tested by Case and Cabalka (2009) at Western Governors University and will be discussed in the following sections.

Plagiarism Detection

Bailie and Jortberg (2008) maintain that due to a limited control over the remote learning environment, institutions have shifted away from secure testing towards project-based or authentic assessment strategies such as written assignments, projects and portfolios. As a result, courses that do not follow a proctored exam route may require students to submit a number of written assignments. The latter, when submitted electronically often scanned for the presence of duplicate content against information available on the world wide web or an assignment database. Free and commercial plagiarism detection tools with a variety of features and degrees of automation are available to institutions. The most accessible way to check a small portion of a written assignment is to use

a free popular search engine such as Google or Yahoo. However, the size of the search query is limited to a few hundred symbols and therefore, this method is not practical for scanning more than a short paragraph at a time. Larger text queries may trigger an error, since search engines are not designed to evaluate large amount of text. One of the popular choices of plagiarism detection tools employed by a large number of universities is Turnitin. This will be discussed in greater detail in the following sections.

Testing Software Biometric Authentication at the University of Maryland University College

University of Maryland University College (UMUC) "is one of eleven accredited, degree-granting institutions in the University System of Maryland (USM)". Founded in 1947, UMUC is the largest public university in the United States. In 2008, UMUC had over 189,000 online course enrollments. Offering a broad range of classes, UMUC has earned a worldwide "reputation for excellence as a comprehensive virtual university and for focusing on the unique educational and professional development needs of adult students" (University of Maryland University College, n.d.). In this pilot project that took place from July to August 2009, a total of 30 participants (27 students and 3 faculty members) volunteered to participate in the pilot project and complete authentication by using signature or gesture biometrics that does not require any specialized hardware. Participants were asked to visit a website that was created specifically for the pilot project, watch an instructional video, create biometric signature profiles and practice validation using their biometric signatures (Biometric Signature ID, 2009). Participant surveys were also administered to assess the overall user experience. "The final exam was administered over two days and at four different exam start times. Student participants were asked to validate their identity using BioSig-ID prior to taking their exam. Students were directed to a bank of separate computers and asked to validate their identities using UMUC supplied workstations and PC mouse(s)". The results show that participants successfully completed authentication using biometric technology as follows: "100% enrollment achieved

for all 30 participants… Average enrollment time of 48 seconds for BioSig-ID and 28 for Click-ID…[and] 97% [of participants] would recommend BioSig-ID be used for student identity verification" (Biometric Signature ID, 2009, p. 8).

Evaluating Software Only Biometrics at University of Texas

A more detailed study of BioSig-ID was conducted by McNabb and Maynard (2010) in partnership with the University of Texas System TeleCampus (UTTC). The results confirm a smaller pilot with the University of Maryland University College (UMUC). "That effort, with 25 students completing a feedback survey, also found high levels of student satisfaction" (McNabb & Maynard, 2010, p. 11). The pilot project was designed to examine student acceptance of the use of software only biometric authentication technology and optimize the student enrollment process.

The pilot study was conducted during a period of five weeks in spring of 2010 "167 students enrolled in online courses offered by nine campuses within the University of Texas System" to evaluate their acceptance of the biometric authentication technology. "Ninety students completed enrollment and ten validations and were asked to complete a feedback survey. Eighty-one percent did so… [N]early all (99%) of students who completed the pilot had positive feelings about the experience…Participating students thought the system was very easy to use…[and] appreciated its value in increasing security" (pp.2-12). McNabb and Maynard (2010) note that the process of enrollment and validation is fast.

Remote Proctoring Program at Western Governors University

Case and Cabalka (2009) conducted a study to test the overall reliability of delivery, as well as the technical constraints associated with successful delivery of the remote proctoring system designed by Kryterion Inc. The pilot lasted two weeks and was conducted in partnership with Western Governors University (WSU). WSU is a non-profit competency based online institution. It is "dedicated to improving access to postsecondary educational opportunities for students that are traditionally classified as underserved. As a fully online institution, students interact with content and assessment remotely, which presents a number of

challenges to assessment" (Case & Cabalka, 2009, p. 1). Kryterion Inc. is a software development company with a long history of experience, expertise and innovation in secure test development and delivery. A wide variety of educational institutions and other organizations have been using Webassessor, the foundation of the Kryterion's testing system according to Kryterion (n.d.). Although WGU employs a wide range of different assessment types, "the two primary methods relied upon most are the proctored objective exam and the unproctored performance assessment… In an attempt to address a number of the issues associated with delivering secure, reliable assessments to a distributed student population, WGU executed two pilots of Kryterion's online proctoring system" (Case and Cabalka, 2009, pp.1-3).

Webcams were installed at each workstation in the test center to monitor student activity. Approximately half of the students scheduled to take assessments in the WGU test center were monitored via onsite proctors as well as online proctors. The remaining students were monitored only via onsite proctors. "A total of 112 administrations were delivered via this method", where a group of 57 students received computer mediated and onsite proctoring and 55 students received onsite proctoring only. "Both quantitative and qualitative data was collected on the time necessary for beginning the administration, issues encountered during the administration, the number of potential procedural violations detected, the overall time taken on the assessment, the scores on the assessments, and student feedback following the administration" (Case & Cabalka, 2009, p.3).

"The second pilot was designed to determine the effectiveness of the system in a distributed, less controlled setting" (p. 3). Two hundred students volunteered to participate in the pilot that spanned one month and were provided with web cameras at no cost. "Measuring the reliability of the system in detecting procedural violations required a baseline, which is why we chose to proctor 50% of the students via online proctoring and onsite proctoring, and 50% via onsite proctoring alone. Only 4 procedural violations were detected during the initial pilot… In two cases, the student moved the webcam. In one case the student was

detected talking during the administration, and in one case a student was discovered attempting to navigate away from the testing webpage to a different URL. The first three procedural violations occurred in the online proctoring and onsite proctoring group while the last procedural violation occurred in the onsite proctoring-only group" (Case and Cabalka, 2009, p.4).

The results of the pilot suggest that online proctoring is at least as effective at detecting procedural violations as onsite proctoring, that authors consider as a "potential advantage" of the online proctoring system (p. 5).

Literature Review Summary

Plagiarism and cheating appear to be the most dominant issues discussed in the literature. Some scholars consider prevention a policy issue (Isa et al., 2008; Sheridan et al., 2005) while others (Mott, 2010; Kennedy et al., 2000) argue for a technology-based solution. Some scholars including Chiesl (2007) suggest a pragmatic approach that minimizes competition among students and changes the process of assignment and exam administration.

The literature also discusses identity control measures employed by institutions that range from onsite proctoring to computer mediated proctoring and biometric authentication. However, one should be particularly cautious about applying traditional assessment methods to distance education as they may outweigh the benefits of distance learning. For instance, distance students may be required to travel to an approved testing center to complete course assessment and universities may impose additional costs for using examination facilities and covering technology and proctoring costs. In the case of technology based authentication, security, privacy and accessibility are significant issues to consider. The research on biometric identity control applications is primarily concerned with user experiences. Further research is needed to assess its effectiveness in deterring cheating or academic misconduct. Without a process that aligns student virtual identities with the academic work they do, the credibility of legitimate universities offering distance courses and programs may not be perceived as credible as that provided by traditional institutions.

CHAPTER III - THEORETICAL FRAMEWORK

Characteristics of Case Studies

There are different types of case study methodology. Baxter and Jack (2008) use seven terms to describe them. They are: explanatory, exploratory, descriptive, multiple case studies, intrinsic, instrumental and collective. For the purposes of this research, a descriptive multiple-case study design was selected as it investigated differences between the five cases. Neuman (2006) points out that:

> Case study uses the logic of analytic instead of enumerative induction. In it, the researcher carefully selects one or a few key cases to illustrate an issue and analytically study them in detail. He or she considers the specific context of the case and examines how its parts are configured… The logic of the case study is to demonstrate a casual argument about how general social forces shape and produce results in a particular setting. (pp. 40-41)

Multiple Case Studies

A multiple case study methodology allows the researcher to examine differences between multiple cases. Baxter and Jack (2008) maintain that "if a study contains more than a single case then a multiple-case study is required… In a multiple case study, we are examining several cases to understand the similarities and differences between the cases" (p. 550). Yin (2003) describes how a multiple case study either, "(a) predicts similar results (a literal replication) or (b) predicts contrasting results but for predictable reasons (a theoretical replication)" (as cited in Baxter & Jack, 2008, p.550). They also maintain that in case studies, as in any other qualitative type studies, the data collection and analysis occur concurrently.

Building Theory from Case Study Research

Eisenhardt (1989) points out that initial definition of the research question is critical in developing theory from case studies. "Theory-building researchers typically combine multiple data collection methods. While interviews, observations, and archival sources are particularly common, inductive researchers

are not confined to these choices" (p. 537). Eisenhardt (1989) maintains that the process of building theory from case study studies is an iterative one and further notes on the case study approach:

> While an investigator may focus on one part of the process at a time, the process itself involves constant iteration backward and forward between steps. For example, an investigator may move from cross-case comparison, back to redefinition of the research question, and out to the field to gather evidence on an additional case… [The process of inductive theory building], attempts to reconcile evidence across cases, types of data, and different investigators, and between cases and literature increase the likelihood of creative reframing into a new theoretical vision. (p.546)

Epistemological Perspective

This study was undertaken using a pragmatic paradigm with an aim to implement findings and conclusions into policies and practices that may help university administrators deal with academic integrity issues. "To a pragmatist, the mandate of science is not to find truth or reality, the existence of which are perpetually in dispute, but to facilitate human problem-solving" (Powell, 2001, p. 884). Tuli (2010) maintains that "[w]hether consciously or not, every researcher works from some theoretical orientation or paradigm" (p.102). "Paradigms thus define different views of the social world based upon different meta-theoretical assumptions with regard to the nature of science and society… Though pragmatism is fairly recent compared to the other philosophical positions, it has positioned itself as a contending paradigm" (Pansiri, 2005, pp. 192-196). Consistent with a pragmatic paradigm, the study includes multiple methods that provide both qualitative and quantitative data to help answer the research questions. The results represent practical operating conditions of five large universities providing remote students with access to learning resources as well as testing and examination facilities. This study provides an opportunity to learn from the best practices and reflect on challenges that institutions of higher education encounter in establishing remote students' identities.

CHAPTER IV - DESIGN

Research Design

This study was undertaken using a multiple case study approach, which is concerned with discovering common patterns across cases. Baxter and Jack (2008) note that if a study examines more than one case then a multiple-case approach should be taken. “In a multiple case study, we are examining several cases to understand the similarities and differences between the cases” (p. 550).

Context for the Research

The five leading universities, in three countries were selected for this study. This multiple case study examines the cases of Athabasca University, Open University UK, Penn State University World Campus, University of Maryland University College and eConcordia– Concordia University's distance learning facility. These institutions fit the criterion of officially accredited universities that offer distance education courses and programs. Each institution has already implemented or evaluated an identity control strategy. Since the scope of this study is limited, only five cases were chosen for the research.

Athabasca University is a publicly funded university located in Athabasca, Canada. It serves over 38,000 students and “offers over 900 courses in more than 50 undergraduate and graduate programs in a range of arts, science and professional disciplines”. The school employs over 1,300 faculty members and staff. It is a distance education institution. To address the student authentication issue, the school has established an Exam Invigilation Network. (Athabasca University, n.d.)

Open University UK is a distance education institution. It is the biggest university in the United Kingdom with more than 250,000 students. The school employs more than 1,200 full-time academic staff. The university is privately funded. The university has established an Exam Invigilation Network for authenticating work of its distance students. (The Open University, n.d.)

University of Maryland University College commonly referred to as UMUC is a distance education institution founded in 1947 and headquartered in

Adelphi, Maryland, United States. The school is “serving more than 90,000 students worldwide” (University of Maryland University College, n.d.). A software biometric authentication project was successfully conducted by the institution. To address the student authentication issue, the school has piloted a variety of authentication technologies.

eConcordia is a distance learning extension of Concordia University a traditional and government accredited post secondary institution founded in 1974, located in Montreal, Canada. In 2002, the distance learning extension was established, providing access to all online courses at Concordia University. It currently offers “60 credit courses from all four Concordia University faculties” (eConcordia, n.d.). It is the exclusive provider of online learning at Concordia University. The university has established an Exam Invigilation Network for authenticating work of its distance students.

Penn State Word Campus is a distance learning extension of Pennsylvania State University (commonly referred to as Penn State) a traditional public research university founded in 1855. It is located in University Park, Pennsylvania, United States. It was one of the first major accredited universities to provide online education. The World Campus was launched in 1998. Remote and traditional proctoring are used for student authentication. (Penn State, n.d.).

Research Population

A total of five officially accredited universities were selected for this research. Athabasca University, University of Maryland University College and Open University UK are distance education institutions. Penn State University and Concordia University are traditional universities that offer a large variety of distance education courses through a distance learning facility. eConcordia is Concordia University's distance learning facility and Penn State World Campus is a distance extension of Penn State University. A strategic convenience sample of university administrative staff involved in development, administration or enforcement of an academic integrity policy was selected.

Publicly available information from university websites was used to generate a preliminary participant list of V.P. Academic and Registrar office staff involved in academic integrity matters. Introductory emails were then sent out to the preliminary list of participants in order to introduce the study and identify the key experts on the academic integrity and in particular identity control issues at each institution. Additional referrals were received, and the final participant list was created. The data from one participant from each university to the total of five participants for the entire study was collected and analyzed.

Participants were selected on the basis of the following criteria:

1. Involvement in development, administration or enforcement of an academic integrity policy.
2. Expressed interest in participating in this research project.

The rationale for choosing to survey administrative staff as opposed to faculty or academic leaders was that the administrators tend to have broader knowledge of academic integrity issues and are responsible for overseeing the entire academic integrity process from policy making to financing to enforcement, whereas other groups tend to have limited involvement and are delegated specialized tasks within the process. Although, faculty and staff share a common understanding of the academic integrity process, the survey results should be interpreted as the opinions of the stakeholder group that is likely to be most informed on the subject of academic integrity. However, a note of caution on this interpretation is appropriate since administrators' opinions may not be widely, and are certainly not unanimously endorsed by all university faculty and staff.

Data Collection Strategies

The data collection process was divided into four phases. First, each university's website was examined for general academic integrity guidelines as well as admission requirements and examination instructions for students. In the second phase of the data collection, strategic convenience sampling was used to select an administrative office staff member from each university and these were invited to answer a brief questionnaire and participate in a follow up interview. A

personal introductory email (see Appendix A) was sent to prospective participants by the researcher to introduce the study and identify the key experts that are responsible for the development, administration or enforcement of the academic integrity policy. During the third phase of the data collection process and once a final list of participants has been established, an introductory letter (see Appendix A) containing a brief description of the study as well as the questionnaire (see Appendix B) was distributed via email. In the final phase of the data collection process, follow up questions were asked through email and via telephone to clarify the questionnaire responses. As well, the participants were provided an opportunity to review, validate and provide additional comments on the conclusions chapter.

Survey Instruments

One survey instrument was developed for this study (see Appendix B). The questionnaire was comprised of seven Liker-like scale questions (with a 5 point range from Strongly Agree to Strongly Disagree) and one multiple choice question. The questionnaire also allowed for qualitative information and extra details to be recorded if the participant wished to provide them. A follow up to clarify the answers was conducted by email or telephone. The data collection was performed using LimeSurvey, a web-based survey software hosted by Athabasca University and via email. Some participants considered it easier to complete the survey via email. Each participant was assigned a unique participant identification number.

Data Analysis Procedures

Upon collecting the necessary data from documents, surveys and follow up emails or phone interviews, the collected information was organized into categories and cross-compared. Neuman (2006) notes that “qualitative researchers often use general ideas, themes, or concepts as tools for making generalizations“ (p. 459). During the comparison stage, data were processed through three types of coding as follows:

Open coding was used to identify emerging patterns and themes and tentatively organize the data into categories. “Open coding brings themes to the surface from deep inside the data” (Neuman, 2006, p. 461). The second phase of the analysis involved axial coding, which examined categories to find links and patterns and generalize them into theme patterns. “When the theme reappears in different places, the researcher makes comparisons so he or she can see new themes” (Neuman, 2006, p. 462). The last phase of the coding process involved drawing comparisons of previously identified themes, through selective coding. “During selective coding, major themes or concepts ultimately guide the search. You recognize specific themes identified in earlier coding and elaborate on more than one major theme” (Neuman, 2006, p. 464). Data analysis was concluded with analytic comparison. “[A] researcher identifies many factors for a set of cases, sorts through logical combinations of factors, and compares them across cases… The real strength of analytic comparison is that it helps researchers identify the combination of factors, often measured at the nominal level, that are associated with outcomes among a small number of cases” (Neuman, 2006, p. 471).

Pilot Study

This research commenced with a single case study, analyzing Open University UK general academic integrity guidelines and learner authentication strategies. The pilot study was to test the validity and utility of the research questions, the logistics of data collection and the data analysis procedures. The results of the pilot study were better than expected. The Open University UK administrative staff were eager to participate in the study and prompt to complete the questionnaire, answer emails and provide additional information.

Conclusion

This study calls for a new organizational strategy to address academic misconduct and identity control measures such that minimize opportunities for identity fraud in a distance education environment. It examines the identity control strategies employed by Athabasca University, Open University UK, Penn State University World Campus, eConcordia and University of Maryland

University College such that address the issue of learner authentication in distance mode. One may argue that with the growing popularity of distance education programs, officially accredited universities have a moral obligation to exercise due diligence and establish protocols that verify learner identity during examination and testing. This is not only important for preserving the perceived credibility of the institution but also for the public safety as may be the case with the critical areas such as aviation training or health care studies. A descriptive multiple case study design was selected for this study in order to examine the differences of institutional level identity control strategies, their effectiveness and challenges as well as identify barriers to their implementation from the perspective of university administrative staff. The participants were selected using a strategic convenience sampling method. They were invited to answer a brief Likert-like scale questionnaire via email or online and participate in a follow up email or phone interview.

CHAPTER V – RESULTS

This study examines the differences of institutional level identity control strategies, their effectiveness and challenges as well as identified barriers to their implementation from the perspective of university administrative staff. The questionnaire was comprised of seven Likert-like scale questions (with a 5 point range from Strongly Agree to Strongly Disagree) and one multiple choice question. Each question was accompanied by a comment section. The Likert-like scale survey results are reported in Table 1. The survey results are summarized from questions as follows:

Cross Case Analysis

Table 1

Likert-like Scale Survey Responses

Case #	**Case 1**	**Case 2**	**Case 3**	**Case 4**	**Case 5**
Primary Authentication Method	Password, Traditional Proctoring	Password, Traditional Proctoring	Password, Traditional Proctoring	Password, Traditional Proctoring	Password, Remote Proctoring, Traditional Proctoring
Plagiarism Detection Tool	Turnitin, Google	Turnitin, Google	Turnitin	Turnitin, Copycatch	Turnitin
Challenges	Provision of examination facilities	No challenges cited	Provision of examination facilities	Technical issues, provision of examination facilities	Technical issues
Barriers	No barriers reported	No barriers reported	Cost	Cost, complexity	No barriers reported
Questionnaire					

Identity fraud has emerged as an issue at my institution.	Strongly Agree	Strongly Agree	Strongly Agree	Neither Agree nor Disagree	Agree
My institution tracks and trends academic misconduct data.	Strongly Agree	Agree	Strongly Agree	Agree	Strongly Agree
My institution has an adequate system of identifying online students before each project or paper submission.	Agree	Agree	Strongly Disagree	Neither Agree nor Disagree	Disagree
My institution has an adequate system of identifying online students before each final and/or midterm exams.	Strongly Agree	Agree	Agree	Agree	Disagree
My institution has encountered barriers to implementation of identity control measures.	Agree	Disagree	Strongly Agree	Agree	Neither Agree nor Disagree

The identity control measures my institution employs to authenticate the identities of online students are effective.	Neither Agree nor Disagree	Neither Agree nor Disagree	Strongly Disagree	Neither Agree nor Disagree	Neither Agree nor Disagree
The system my institution employs to conduct remote identification of test takers has challenges.	Disagree	Disagree	Agree	Agree	Agree
The best practice for authenticating the work of remote learners is:	Traditional Proctoring / Invigilator network	Traditional Proctoring / Invigilator network	Traditional Proctoring / Invigilator network	Each system has advantages and disadvantages. What is best depends on circumstance, cost and context.	Remote proctoring / Biometric/ Policy Enforcement

Question # 1 Identity fraud has emerged as an issue at my institution. (SA/A/N/D/SD)

There was a general consensus among the surveyed university administrators that the identity control of remote learners poses a concern. One administrator notes “We are starting to receive reports of students hiring others to complete online assignments and quizzes”. This response was expected. It is in line with the literature review. To summarize, the physical separation of learners and instructors and reliance on username and password authentication as the primary means of validation of student identities creates a potential for abuse. One administrator stresses “Students are expected to complete assignments during their studies. These are completed 'at home' where there are no controls over the origination of the responses”.

For the U.S. based institutions, it is also the law that requires implementation of procedures to ensure that “…the student who registers in a distance education or correspondence education course or program is the same student who participates in and completes the program and receives the academic credit” (Higher Education Opportunity Act, 2008). One administrator comments “Due to the reauthorization of the higher education [opportunity] act in 2008 it is critical that distance education providers have a solid solution in place for assuring they know the identities of their students studying online at a distance”.

Question # 2 My institution tracks and trends academic misconduct data. (SA/A/N/D/SD)

The tracking and trending of academic misconduct data is a measure that all of the surveyed institutions employ. One administrator notes “We have a committee made up of faculty members and administrators who enforce the Academic Code of Conduct and track and deal with violations of the code”. Not only instructors but also students may report instances of academic misconduct that are later reviewed and analyzed. This response is in line with the expected response and general overview of academic integrity procedures available on universities’ websites that institutions have a system in place for tracking

academic misconduct trends. It also ties into the answer to the first survey question about emerged instances of identity fraud. The process of reporting and trending academic misconduct data is a multifaceted one and involves a variety of stakeholders. Some cases are handled by instructors, while others may be escalated and dealt with by designated committees.

One administrator responded “Yes all reported instances of academic misconduct or integrity are tracked by the Office of Student Conduct” and in another case the response emphasized disciplinary action as the criteria for tracking: “About 85% of continuous assessment and project end-of module assessment is submitted electronically. Text based submissions are then subject to software analysis to assist with the detection of plagiarism and collusion. This in turn may lead to disciplinary action. The latter is recorded, tracked and analyzed”.

Although tracking and trending are employed by all five institutions surveyed in this study, the analysis criteria and methodology for processing academic misconduct cases may vary. Therefore, academic data tracking is a process that is worth examining further. It is unfortunately outside the scope of this paper. One may assume that such further research may not be without challenges as one participant responded: “We do track the data but it is not publicly disseminated (within or outside of the institution)”.

Question # 3 My institution has an adequate system of identifying online students before each project or paper submission. (SA/A/N/D/SD)

The responses to this question were wide ranging. Two participants perceived the system of identifying online students before each project or paper submission to be adequate (agree), one was uncertain (neither agree nor disagree) and two did not consider the system adequate (one respondent answered disagree and another one strongly disagree). The expected outcome was that the administrators would indicate satisfaction with their system of identification of students before each paper submission, which was not the case. One administrator comments “we are exploring options for how to authenticate students at various moments in each course”. All institutions rely on username and password

authentication for access to a learning management system which provides some confidence in knowing whether or not one has used someone else's login credentials to submit a weekly assignment or a final paper. One administrator notes: "Given recent situations where we have found that students have released their secure log in information to others for the purposes of completing online assignments and quizzes, strongly disagree has been chosen".

Some institutions put greater emphasis on technology such as plagiarism detection tools, and analysis of login patterns, while others rely on student-instructor relationships for the detection of irregularities in students' work; and there are also those that strive to balance technology with traditional assessment methods. One administrator comments "Each student has a unique log-in and password and we can check for I.P. sharing, time of log-in and log-out, but there is no way of telling that the individual is who they say they are when they submit their assessments" and in case of another institution the response was: "We rely on the instructor to form the relationship with the students so when they review a paper or project they can detect an irregularity in the quality and style of work. Many courses stage the projects throughout the course. For example, in the second week, the thesis statement is due. In the third week, the annotated bibliography is due. In the fifth week a rough draft is due. Each stage includes feedback and discussion with the instructor- so the students are required to interact and discuss the project". Instructors indeed add another layer of identity assurance. Many online courses involve an interactive learning and participation often through online discussions, web or telephone conferences. Learners demonstrate academic skills throughout the course allowing instructors to track their progress and flag any suspicious activities or question the origin of the submitted content. "Most assessment tasks that are submitted in hardcopy are a consequence of the need to use symbols that are expensive and/or complex to use on screen eg. mathematics and music. With hardcopy submission we are reliant on the judgment of the markers to identify misconduct".

Assignments that are submitted electronically, often screened by instructors for plagiarism, using plagiarism detection tools. In one case, the

screening process was described as somewhat ad hoc: “[plagiarism and collusion detection tools are] not standardized. Some faculty members use Turnitin. We are currently working on an institutional policy in respect to use of plagiarism detection software”. Turnitin was cited in all five cases and Copycatch was used by one institution. Google search engine was also occasionally used by some instructors as a first line of defense against plagiarism. In one case the administrator comments: “We use Turnitin. Also, unofficially, some instructors use a Google search for first detection”.

Question # 4 My institution has an adequate system of identifying online students before each final and/or midterm exams. (SA/A/N/D/SD)

Four out of five administrators consider the system of identifying online students before each final and/or midterm exam adequate. The expected response to this question tallies with that received. Unlike paper and project submissions, exams are treated with higher scrutiny. They often rely on traditional verification measures, such as proctored exams where proctors verify officially issued identification before students can take the exam. This method of student authentication may be considered the safest available alternative to learner authentication since it has been widely employed by traditional institutions. However, even physical verification of personal identification is not without challenges. In one case the administrator notes: “Students are required to present a government issued photo ID to an invigilator before writing an exam. Having said that, there have been a handful of cases over the years of students being in "cahoots" with their invigilator, so the potential of cheating is possible”.

Another interesting finding is that there is the variance in institutions’ preferences for conducting proctored exams. Institutions are striving to balance alternative non-secure methods of assessment with traditional ones as one administrator notes: “We are piloting several different methods of authentication. We also count on the instructors to notice irregularities in the student's language and abilities among class discussions and projects. Many of our classes use project-based assessments rather than traditional exams”. In one case

administrator comments: “All final exams are done in-person or, if at a distance, via a proctor. Final exams are usually worth at least 50% of the final grade because of the fact that it is the only assessment where the identity is confirmed” while in case of another institution, the response was: “Only a small number of exams are proctored face to face these days. Most of our courses have moved to authentic assessments/projects or ‘take-home exams’. We do have a number of timed exams and we are piloting a software service called fast test web” and yet a third case noted that “[a]bout 50% of modules have an end-of-module examination. Student ID is checked at the beginning of each examination by the invigilators”.

Question # 5 My institution has encountered barriers to implementation of identity control measures. (SA/A/N/D/SD)

The responses to this question do not point in one specific direction. The surveyed universities have established procedures for authentication of remote learners and their perceived effectiveness will be discussed in the following sections. The traditional proctoring method and password protection of the learning management system are employed by all of the five institutions (see summary in Table 1). One university is using a remote proctoring solution that combines both video surveillance and software biometrics. Some of the surveyed institutions are satisfied with the outcome, while others are piloting or have already examined various initiatives to further strengthen authentication measures. At the time of this writing, two institutions are evaluating new authentication initiatives. In one case, the administrator comments that “[t]here have been no barriers. We are just trying to figure out which method/product is best given resources and characteristics/needs of the students” while in another case, the outcome of a technology based solution was less comforting. The administrator notes that “the software has not provided the level of confidence that we need in terms of reliability and security”.

The expected response to this question was that the administrators would unanimously cite cost and complexity as the primary barriers to implementation of identity control measures. As well, organizational issues such as a resistance to change were expected to be discussed. However, this was not the case. High cost was cited as a barrier to implementation in only two cases. One administrator maintains that "[o]nline biometric control technology is expensive and beyond the reach of most post secondary institutions i.e.; finger print or facial recognition process". Not only the initial deployment of technology is expensive, but also its maintenance and administration may require additional resources. This in turn may affect student tuition costs that could be raised to offset the investment. Another administrator comments: "The issues are to do with cost and the complexity of implementing new technologies in remote centers". One case reported positive attitude towards change by the faculty: "No this has not been the case as most faculty are in favor of knowing that students are doing their own work and that we can track and document such".

Question # 6 The identity control measures my institution employs to authenticate the identities of online students are effective. (SA/A/N/D/SD)

Four out of five administrators were uncertain (neither agree nor disagree) about the effectiveness of the identity control measures employed by their institutions, and in one case these measures were perceived as ineffective (strongly disagree). Overall effectiveness ultimately depends on institutions' ability to authenticate student work at various stages in a course with a reasonable degree of certainty, and that is a challenging task. Institutions do employ a variety of authentication strategies for some of the course components, they track academic misconduct data in addition to policy enforcement and education, and yet the dominant method of student authentication remains to be the classic password protection. One administrator notes: "[the methods are effective] probably only partially as students are not supposed to sign on for others or give out their user IDs and passwords (this is a policy and a statement that all students sign). However, there is no way to actually monitor this". In another case, the

password authentication is also cited as a possible reason for limited effectiveness: “On-line identity is password and system controlled. This does not prevent collusive impersonation”.

This was not an expected response. The answers to the previous questions show that institutions track academic misconduct data, maintain exam invigilator networks, validate electronically submitted assignments for plagiarism, and also some of the schools surveyed do not perceive barriers to implementation of identity control measures. This suggests that they are in control of the remote authentication process and should have a good understanding of whom their students are. However, this is not what the survey results suggest.

Question # 7 The system my institution employs to conduct remote identification of test takers has challenges. (SA/A/N/D/SD)

On the subject of challenges, associated with the identification system of remote test takers, opinions were split. Three university administrators reported having logistical, administrative and technical challenges with their systems of remote learner authentication while the remainder cited no challenges. The quality of examination facilities, scheduling procedures and related service fees vary depending on location. As a result, management of examinations and invigilator validation to ensure the remote facilities and examination process is in compliance with the institutional standards often becomes a resource-intensive task. One administrator comments: “Operational and logistical challenges exist, primarily in the area of invigilator availability and extra fees charged to students. Verifying invigilator eligibility in accordance with our standards is also quite time consuming”. Another administrator notes that “[f]inding an adequate location is sometimes a challenge, but for the most part, it has worked out”. Time zone differences contribute to logistical challenges. This was cited in one case. Administration of a standardized test in multiple time zones is a risk factor in itself because test answers or any information that can jeopardize test integrity could be shared online right after or even during the first exam but before the

second one commenced, leaving enough time for shared information to be reviewed.

Since not all examination facilities are managed equally and offer the same level of service and support infrastructure, technical issues may arise. One administrator notes: “We use many different organizations for the provision of examination rooms/halls etc - in general these are not specialist facilities and only rarely do they have good provision for electricity supply for laptops/PCs, etc. and even more rare is network connectivity”. Technical difficulties were also cited in case of remote proctoring. Technology based authentication entails many complexities and issues such as software compatibility and network connectivity. One administrator comments: “it is still fairly new and depends on several pieces of technology working in unison, it still sometimes has technical glitches. However, this is true for any technology we employ in our courses as many are trying to keep up with the rapid evolution of browsers and other services like Flash”.

The survey responses were consistent with that expected. The provision of examination services to a large number of students widely dispersed over a large geographical area is a challenging task and may result in logistical, administrative and technical issues. What was interesting about these responses was that university administrators referred to proctored examinations as the primary means of student authentication. One would expect discussions regarding challenges with monitoring student login credentials and IP addresses, learning management systems or challenges with enforcement of institutional policies, but this was not the case. The emphasis was placed on examinations. Another interesting finding was that not all examination facilities contracted by universities were specialized or equipped with sufficient support systems such as electrical outlets and computer network connectivity. One would expect a consistent application of technical requirements from all providers of examination facilities.

Question # 8 The best practice for authenticating the work of remote learners is:

The participants were presented with four multiple choice options of authentication methods as well as an opportunity to add additional methods and comments. The presented choices were as follows:

A. Remote proctoring using web cams.
B. Biometric authentication asserting the identity of the student by fingerprints, keyboard activities, etc.
C. Traditional proctoring.
D. Policy enforcement.
E. Other.

Traditional proctoring was reported to be the best practice for remote learner authentication, by three out of five (60%) surveyed university administrators. This long-established examination method bridges the gap between virtual and physical identities of remote learners and has been serving well the traditional institutions. One administrator comments: “I think face to face is probably the only way to be 100% sure that the learner is who he/she says. I think the other methods can be tricked by our more creative learners”. As it was cited previously, the proctoring process is not without the challenges and may bring about logistical, administrative and in some cases security issues. However, its benefits should not be ignored as one administrator stresses that traditional proctoring is “[c]heaper for the student, proven practice, and not limited by time-zone differences for web cam authenticating”.

In a separate case the administrator suggests “[g]iving larger weight to proctored exams where students are required to present photo ID seems to be most effective. While this method still presents potential issues, those issues are minimized”.

Although traditional proctoring is perceived favourably and employed by all five universities reviewed in this study, it is not consistently employed across all courses and programs as a standard method of learner authentication. Non-secure evaluation methods such as projects, portfolios and assignments that do not always align student physical identities with their virtual ones are often used in

lieu of secure examinations. Only one institution reported proctoring all of the final exams. That is one hundred percent of students show their official identification cards before each final exam. The administrator stresses that "[a]ll final exams are done in-person or, if at a distance, via a proctor. Final exams are usually worth at least 50% of the final grade because of the fact that it is the only assessment where the identity is confirmed".

In the remaining two cases, a combination of technology based strategies and policy administration were cited: "Remote Proctoring using web cams, Biometric Authentication asserting the identity of the student by fingerprints, keyboard activities etc. Policy Enforcement. The best approach is a combination of the above items listed. Also, none of these systems are adequate if a student is only taking a single course. Where they become powerful is when they are used across a program and several courses". Another administrator notes that "[e]ach system has advantages and disadvantages. What is best depends on circumstance, cost and context".

The expected response was that the administrators would be inclined to suggest a technology based authentication solution, but this was not reflected in the survey data. Quite to the contrary, proctoring either traditional or remote was cited in the majority of cases (80%). What is more surprising is that administrators at institutions that piloted various authentication technologies consider traditional proctoring to be the preferred alternative to student authentication and at the same time continue using non-secure evaluation strategies in lieu of secure proctored exams. Further research in this area is required to explain the discrepancy between the perceived measures and the ones employed.

CHAPTER VI - DISCUSSION

The findings from this study tend to reinforce the idea that the values and standards of academic integrity remain the same regardless of the medium of instruction. One may argue that a project paper or assignment collected by a teaching assistant in a large auditorium of a traditional school, provides the same level of identity assurance as the one submitted electronically. Neither identity of students nor authorship of manuscripts is validated with a high degree of certainty at the time of collection. Students are expected to be honest across all academic activities they participate in whether in class or online. The issue of trust is key, however one may not merely rely on an assumption that the virtue of integrity is maintained by all students. There are examples that speak to the contrary ranging from ghost writers to off the shelf papers to identity fraud rings. Identity control measures are not only important for preserving the perceived credibility of the institution, but also for the public safety as may be the case with the critical areas such as aviation training or health care studies. Therefore, authentication is justified and ought to provide a system of checks and balances that ensures that the relationship of trust is intact. One may argue that it is not only the type of authentication that promotes academic integrity as some provide greater security features than others, but also that it is standardized and consistently applied.

Learner Authentication

Learner authentication is comprised of two dimensions: learner identity and authorship of academic work produced by a learner. A learner authentication model is depicted in Figure 1. For authentication to be complete both dimensions of identity and authorship need to be confirmed. While some strategies are well suited for identity assurance in an online environment, others are ineffective in validating authorship regardless of instructional medium. Authorship validation depends on identity authentication as credit needs to be assigned to an entity. It is impossible to confirm authorship without a valid author. Thus, authorship without identity cannot exist. Proctored exams, both traditional and remote using multi-biometrics, confirm not only one's identity through validation of documents or

comparing biometric data to the previously created identity profile, but also authorship of any academic work produced during the proctored session. Provided that proctoring and initial identification of participants was conducted effectively and accurately.

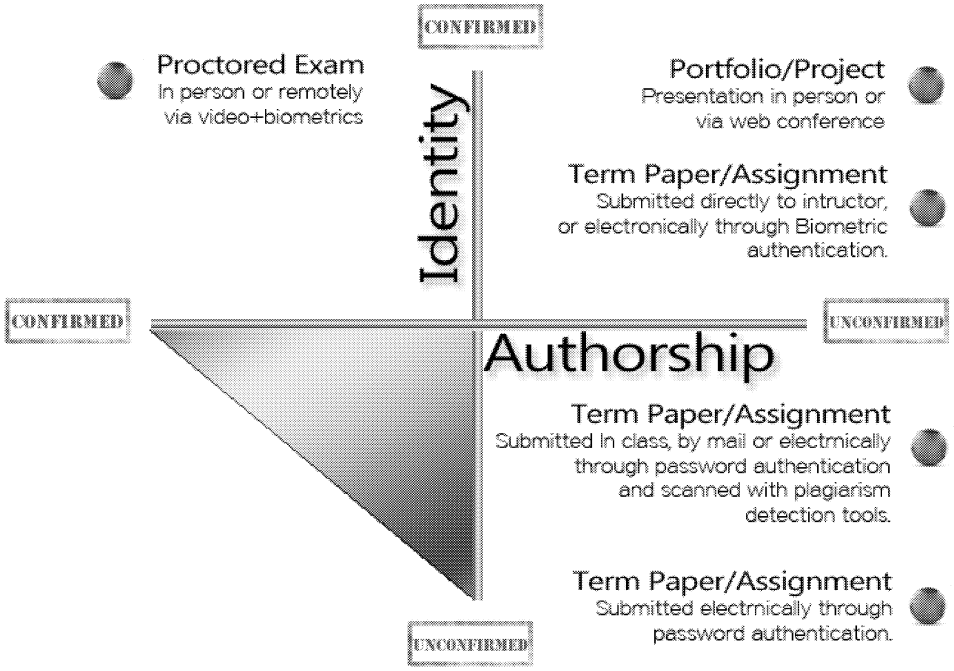

Figure 1. Learner authentication model.

In case of a project or portfolio where an oral defense or presentation is required as a part of the authentication process and conducted in person or via a web conferencing system, only student's identity can be confirmed. Validation of authorship of any work produced prior to the meeting is going to remain a relatively challenging task. Plagiarism detection tools may only detect the presence of plagiarism in materials submitted and therefore ineffective in establishing authorship. However, instructor validation may address just that. Instructors that validate student progress throughout the course should be able to flag any irregularities in students' work and question them. Similarly, assignments submitted through biometric authentication systems validate learner identities, but not their authorship. Term papers, forum discussions, assignments, take home

quizzes and independent research projects submitted electronically using password authentication, through a learning management system or email score low on both dimensions. Plagiarism detection tools are not designed to either validate authorship or identity, but to flag any duplicate content found in its database. Once again, the onus may be placed on instructors to conduct student authentication the traditional way and compensate for shortcomings of technology. However, recent developments in computer science are highly promising for addressing the challenges of authorship identification. A study conducted by Iqbal, Binsalleeh, Fung and Debbabi (2010) examines the framework for extracting a unique fingerprint called "writeprint" from text by anonymous authors. In a similar study conducted by Zheng, Li, Chen and Huang (2006) the results of the experiments suggest that it is possible to identify the authors of internet messages written not only in English but also Chinese, with an accuracy range between 70%–95%. Although, these studies were aimed at establishing authorship of anonymous e-mails or newsgroup messages, these frameworks can potentially be applied to other text sources such as electronically submitted assignments, projects or presentations. This technology could prove to be beneficial for administration of Massive Open Online Courses (MOOC). Many leading universities including Stanford University, Harvard University and Massachusetts Institute of Technology promote accessibility and lifelong learning by offering free online non-credit courses to anyone with the internet connection. MOOCs attract thousands of students from around the world. Due to high the volume of enrollments, examination and testing are automated and are based on only password authentication. The advancement of authentication technologies such that validate authorship and identity may one day bring MOOCs to the level of for-credit courses.

It may seem that one who criticizes distance education on the basis of comparison to traditional education and promotes proctoring as a mandatory component of a distance course, commits the naturalistic fallacy, trying to derive 'ought' from 'is'. If secure examinations are employed by traditional schools, therefore distance education ought to follow this route. However, this is not the

case as not all authentication strategies deliver equal security measures (see Table 2) and proctored exams are generally treated with higher scrutiny. Authentication hierarchy is depicted in Figure 2. Therefore, proctoring as a means for secure examination provides a valuable advantage. Administrators perceive adequacy of identifying students before final and/or midterm exam higher (80%) than that of a project or paper submission (40%). And four out of five administrators (80%) consider proctoring as the best practice for remote learner authentication.

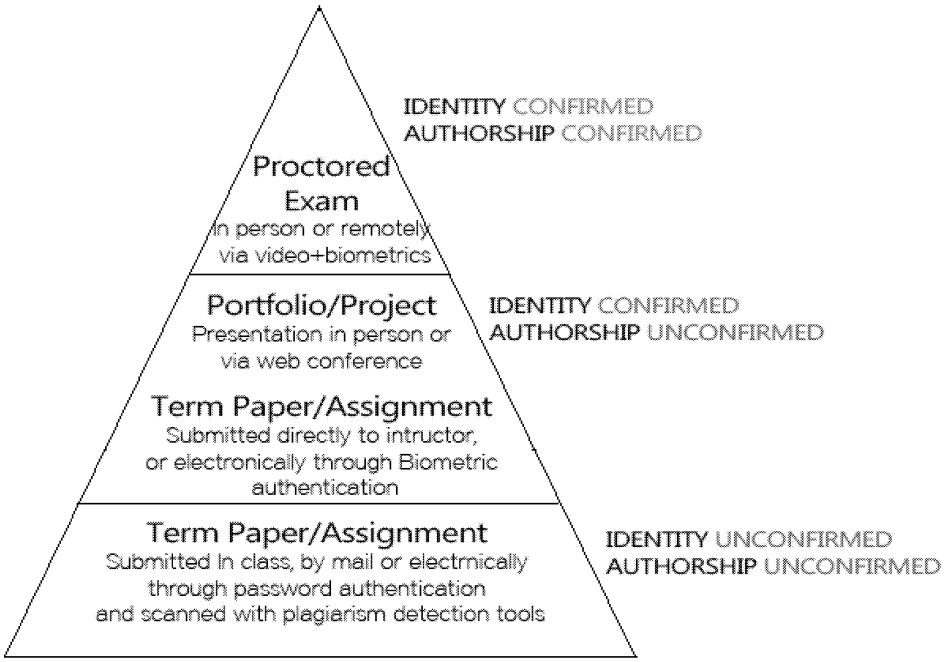

Figure 2. Hierarchy of authentication measures.

Remote Proctoring

Remote proctoring is conducted by trained proctors through video and audio monitoring using wide angle web cameras. It is often used in combination with biometric authentication as well as software that disables certain features of computer operating systems, limiting user access to only educational resources approved for examination purposes. All other functionality and access to the internet is blocked to avoid plagiarism, collusion or any cheating attempts. The survey results show that traditional proctoring is not an exception and is also

prone to incidents of cheating or collusion between proctors and students. One may argue that remote proctoring minimizes the likelihood of two parties being in "cahoots", as they are physically separated and have little opportunity to interact. The chances of them knowing each other before the exam are very slim as proctors may be located in different cities or countries.

Biometric Authentication

Each biometric measure is unique to the individual and unlike username and password authentication is more difficult to share and duplicate (Levey & Maynard, 2011). However, this technology is also sensitive to changes in user's physical condition. For example, a sports injury may affect one's ability to use a computer keyboard and complete keystroke authentication. A secondary biometric key may act as a fail-safe mechanism or provide an additional layer of identity assurance. Multi-biometric authentication entails even higher level of security as it requires validation of more than one biometric key. The most important step in this process is the identity enrollment. It entails creating a biometric profile that is registered against validated identification such as officially issued documents, thus assigning biometric data to a name or identification number. "In its truest sense, this is an assurance that an individual presenting himself as Bill Jones actually is Bill Jones… Identification activities begin with the collection of personal information used as further proof of identity, including facets such as legal name and address, social security number, academic records, and so on. Subsequent to formal enrollment, online students are issued a token (such as a user name) to be used as an identifier to access a secured online course" (Bailie & Jortberg, 2008, p.66).

One may argue that the very process that promises secure authentication of distance learners is also a barrier to accessibility. In order for a student to enroll at university and create a secure student profile, university must provide assistance to facilitate digital identity enrollment, either internally or rely on external service providers. It may work well for local institutions, but in case of international students enrolling in a single distance course in another country or in

a city that is not within driving distance, the logistics of student registration and validation of officially issued documents poses a serious logistical challenge.

Self-enrollment provides necessary convenience and improves accessibility; however, it undermines the very premise of security. Already, many universities adopted an automated admission process that simplifies file management, where prospective students complete admission applications online. In most cases, transcripts are the only original documents that are required for admission, whereas identification documents may be requested in cases where financial aid, confirmation of domestic tuition rates or issuance of students IDs are involved. Biometric authentication entails that all distance students dispersed over large geographical area would need to confirm their identities using original, officially issued identity documents. One may argue that it may become a barrier to implementation. There is a growing selection of government issued enhanced documents with embedded biometric data. These include passports and drivers licenses. And as their availability increases, biometric authentication may become as common as password authentication.

None of the surveyed institutions employ biometric-only authentication of remote learners for the purposes of access to the learning management system or academic resources such that replace or compliment the username and password authentication. Traditional proctoring however, may be argued to be a biometric authentication process in its primitive form, where human proctors scan and analyze facial features of examinees against their identity documents. As it was discussed in the literature review section, this process is not always effective, and male imposters have been admitted to write exams in lieu of female examinees. Access to online academic resources such as email, electronic libraries and learning management systems remains predominantly dependent on password-based authentication. This method of authentication is also the one that provides greatest accessibility to distance education. The implications of biometric authentication on institutions and students lie not only in accessibility but also may result in a possible shift of academic misconduct. Since institutions will be able to validate learner identities using biometrics with greater certainty, the

identity fraud issue may be eradicated or replaced by that of collusion or plagiarism. It will be the authorship dimension of authentication model that would still require validation.

Accessibility

The importance of accessibility in distance education is an issue frequently discussed by many scholars. Bates (2005) stresses that:

> learning will not occur if learners cannot access the technology… For a highly selective research university it may be acceptable to mandate that all student must have a laptop computer. However, an open university needs to accommodate learners denied access to conventional institutions... Thus, an open institution needs to use technologies that are already easily available to all its potential students… Home access to technology will often be the most convenient for distance learners and the most economical delivery location for institutions. (pp. 50-52)

With greater pressure to enhance security of learner authentication, the openness of open learning is challenged and may change as we know it.

Organizational Issues

Logistical and administrative issues were reported among the challenges facing administrators for the provision of examination facilities. Technical issues were also reported when technology based authentication was employed. As new technologies emerge, institutions should not only examine the benefits, but also implications on the organizational structure. Bates (2005) maintains that "[s]uccessful technology applications usually require more than just the purchase and installation of equipment, hiring of technical staff, and the training of teaching staff. Successful implementation also requires some major structural or organization changes within an institution. In addition, there are often powerful external factors influencing the decision to use a particular technology, such as government initiatives or high-profile marketing of services by the commercial sector" (p.63).

Bates (2005) adds a note of caution about bias toward new technology. He maintains "it is often easier to get funding for new uses of technology than funding to sustain older but successful technologies. Although audio-cassettes combined with print materials can be a very low-cost but highly effective teaching medium, they are not sexy. It will usually be easier to persuade funding agencies to invest in much more costly and spectacular technologies… There is much risk in being too early into a new technology. Software may not be fully tested and reliable, or the company supporting the new technology may go bankrupt" (p. 65). He further stresses that "[s]tudents are not guinea pigs, and reliable and sustainable service is more important to them than the glitz and glamour of untried technology. Thus it is better to be at the leading edge, just behind the first way of innovation, rather than at the bleeding edge" (p. 65).

CHAPTER VII - CONCLUSIONS

This study was designed to answer the question of what measures universities with large distance education programs employ to align identity of learners with the academic work they do, as well as examine effectiveness, challenges and barriers to their implementation. The research was undertaken using a multiple case approach and examined survey responses from academic administrators at five officially accredited post secondary institutions in three countries. The data collection was carried out from June to October 2012. The responses were wide ranging and findings will be summarized in the following sections.

Academic Integrity

Identity fraud is an issue that affects all academic institutions and particularly a concern for those that provide service to remote learners. Physical separation creates the gap of anonymity. One administrator indicated reported cases of students sharing login credentials and hiring others to complete online assignments. Authentication protocols need to be implemented to close the gap and align virtual identities with the work that students do. Access to academic resources and learning management systems is often protected by a username and password authentication. This method is not designed to validate one's identity or authorship of submitted materials, but rather act as a gatekeeper granting access to anyone with the correct user name and password combination. Like a door lock, it prevents unauthorized access, but does very little to examine identities of anyone inserting the key. The problem is serious enough to have drawn attention of the United States Department of Education. In 2008, U.S. Congress enacted the Higher Education Opportunity Act (2008). Section 602.17 of the act requires institutions to develop and employ measures that validate identities of the distance learners.

Policy and Enforcement

All of the surveyed institutions have designated staff to deal with reported incidents of academic misconduct. This process often involves multiple stakeholders. While some cases are handled by instructors, other cases may be escalated and reviewed by designated committees. The reported data are tracked and trended by all five institutions; however, the criteria for tracking incidents and methodology of data collection may vary. A disciplinary action is generally the last resort. Education and communication are more preferred methods of managing academic misconduct cases. Students are provided with academic integrity tutorials and resources, they may be required to sign a statement of academic integrity or complete a quiz. In serious cases, penalties are assigned by designated committees on a case by case basis as the magnitude of an offence may hinge on a number of factors. It often takes a retributive justice approach. Since copy and pasting of a website article is different from uploading a digital image of a final exam taken with a smart phone to the file sharing website, penalty needs to be proportional to the damages caused. Tracking incident data is a vital part of risk management and is a process that is worth examining in itself. This will be discussed in the future research section.

Authentication Strategies

There are several authentication strategies available to universities, aimed at enhancing authentication of student work. These are depicted in Table 2. They also provide different levels of assurance. A course or program may employ any combination of these strategies to manage academic integrity and maximize identity assurance. Some strategies provide a greater degree of confidence in the identification of students than others, therefore classified into two categories. Courses that do not follow the exam route, often employ low-level authentication measures for validation of student identity before a submission of projects, assignments and papers as well as participation in an online discussion groups or completion of an online quiz. They rely on the username and password authentication for access to learning management systems, which provides little

confidence in knowing whether or not one has entered someone else's login credentials to submit a written assignment or participate in a weekly discussion forum. As it was previously discussed in the Learner Authentication Model section, the traditional username and password approach is not effective at confirming neither identity nor authorship for any submitted work.

In order to compensate for limitations of the traditional authentication methods, additional validation measures such as login pattern analysis, instructor validation and plagiarism detection tools are often used. Although, the latter is not an identity control strategy, but rather a method of disproving authorship of any written work, assignments that are submitted electronically are often screened by instructors for plagiarism, using plagiarism detection tools. Turnitin was cited in all five cases, and Copycatch was used by one institution. Google search engine was also occasionally used by some instructors as a first line of defense against plagiarism. At the time of this writing, no commercial writeprint or forensic authorship identification software is available to institutions.

Table 2

Authentication Strategies

Low Level Authentication	**High Level Authentication**
Password Authentication	Proctoring (Traditional)
IP Monitoring/Login Pattern Analysis	Proctoring (Remote)
Instructor Validation (Large Groups)	Instructor Validation (Supervised Study)
Plagiarism Detection (Similar Content)	Plagiarism Detection (Writeprint)

Instructors also play an important role in student work authentication and contribute to identity assurance. Learners demonstrate academic skills throughout the course allowing an instructor to track student progress and flag any suspicious activities or question the source of the submitted content. It may serve as an effective identity authentication and authorship validation mechanism when students' activities are closely supervised and continuously evaluated, such may be the case with supervised research projects where intermediate snapshots of

work in-progress are examined and discussed through telecommunication technologies that replicate face to face communication. Furthermore, a login data analysis may not be effective in aligning student identities with the academic work they do. It is not safe to assume that the variance in login patterns is indicative of a problem, whereas a correctly entered username and password is not.

However, the second list of strategies shares much of the same validation protocols as that employed by the traditional institutions. This usually involves face to face interaction with instructors, validation of officially issued identification documents and participation in proctored exams at designated examination facilities. Technologies that enable synchronous communication such as video conferencing substitute for physical meetings. Even in project route courses, instructors may include interactive participation components, through the web or telephone conference systems allowing students to present and discuss their ideas, research, assignments and conduct thesis defense and oral examination.

Unlike electronic paper and project submissions, exams emphasize higher security measures. Facilitation of exams requires traditional methods of authentication such as verification of officially issued identification. The remote proctoring process follows a similar pattern. When remote proctoring is used outside of the designated test centers, students are required to create a multi-biometric profile comprised of a keystroke signature and a photograph. However, the majority of institutions (80%) use proctoring for only select courses or high end exams. The remainder of courses relies on low level authentication, such as projects, assignments and take home quizzes. Only one school (20%) reported conducting at least one secure examination for every course.

The survey results show that perceived adequacy of identifying students before final and/or midterm exam was reported to be higher (80%) than that of a project or paper submission (40%). Furthermore, four out of five administrators consider proctoring as the best practice for remote learner authentication. Three administrators selected traditional proctoring, and one selected remote proctoring.

Although, proctoring is perceived favourably and offered by all universities examined in this study, it is not the primary learner authentication strategy that is consistently applied across all courses, likely due to costs and management challenges.

Challenges

In distance education environment, academic integrity and technology are interconnected and continuously evolving. New methods of student authentication emerge, so are technologies that facilitate cheating. For some institutions, technology was not able to provide the desired level of performance. For others, high cost of technology created a barrier to implementation. In addition to the cost of technology selection and initial deployment, maintenance, support and administration may exert a significant impact on the budget. This in turn may affect student tuition rates and consequently accessibility.

High level authentication strategies add logistical burden on instructors and administrators. Provision of examination facilities, time zone differences and technical issues are some of the challenges that administrators reported when dealing with exam invigilation both traditional and remote. Examination facilities are managed differently based on location and therefore, there is the variance in level of service and support quality. Non specialized facilities were also reported being used in one case. This was a surprising finding. These facilities did not provide an adequate number of electrical outlets for personal computers or sufficient network connectivity. Facilitation of standardized exams in examination centers dispersed over multiple time zones is also a challenge, as it creates a potential for sharing exam information between learners in different time zones.

Technical issues were also reported emerging outside of examination facilities. Remote monitoring of students' computers that use different operating systems may be affected by compatibility issues. Technical glitches resulting from software or hardware failure or loss of connectivity during examination, may undermine reliability and efficient operation of the remote proctoring.

Nevertheless, the future outlook for secure and reliable remotely managed examination is optimistic.

Effectiveness

An effective authentication system enables aligning student work with their identities with a reasonable degree of certainty at various stages in a course. The survey results show that the effectiveness of the identity control measures employed by the surveyed institutions is not well known. The high-level authentication strategies were not consistently applied. Many courses are designed for authentic assessments and project-based learning and do not always provide an opportunity for identity validation. Only in case of one institution all of the final exams were reported to be proctored, the remainder of participants did not report a consistent application of the high-level identity authentication strategies. While administrators were satisfied with select components of their existing system of authentication, pilot projects or various initiatives to further strengthen authentication measures were underway. Institutions are striving for continuous improvement and examining methods that promote academic integrity and higher identity assurance.

Recommendations

This study was undertaken using a pragmatic paradigm with an aim to implement findings and conclusions into policies and practices that may help university administrators deal with academic integrity issues. A complete avoidance of secure testing is not reasonable. Identity and authorship validation can and should be conducted at various points during a distance course. But to make it possible, administrators and instructional designers need to start taking academic integrity issues into consideration at the course/program design stage and consistently embed high level authentication strategies into the course activities. Unlike nonsecure electronic paper and project submissions, exams emphasize higher security measures. The majority of administrators consider proctoring as a means for secure evaluation. Biometric authentication may also provide a higher degree of identity assurance. Facilitation of secure exams

requires traditional methods of authentication such as verification of officially issued identification, and until technology provides an accessible, cost effective and efficient means of identity and authorship validation, proctored examination should be consistently applied across all courses.

Future Research

This study provides a context for future research questions. The research on biometric identity control applications is mainly concerned with user experiences. Further research is needed to assess its effectiveness in preventing cheating, identity fraud and academic misconduct. As previously noted, institutions put onus on instructors to conduct authentication tasks such as monitoring students' progress and flagging irregularities in their work. A future study may examine the process of validation of students' identities from instructors' perspective and analyze the effectiveness of both the non technical means and technology tools instructors employ. Furthermore, studies on academic misconduct usually report data collected from student surveys. However, self-reporting of dishonest behavior is not without a challenge. Since institutions track and trend academic misconduct data, future research may focus on an institutional level academic integrity incident reporting; and not only compare institutional data collection and analysis procedures, but also examine the magnitude of academic dishonesty and identity fraud in particular.

The impact of secure authentication measures on accessibility is another question that has arisen as a result of discussion about various levels of authentication. Future research may examine accessibility levels of several authentication technologies and evaluate their influence on instructional design considerations and distance education in general. There is a discrepancy between what administrators consider effective measures of authentication and what measures they employ. A future research may examine this gap. And to conclude with a more fundamental question, a future study may examine different perspectives on what is perceived a reasonable degree of certainty for authentication of student work. Should distance education schools follow the

footsteps of traditional institutions and conduct at least one proctored exam in every course or continue relying on username and password authentication ? Finally, the use of high stakes examinations as a corner stone for academic integrity is itself under challenge. Is performance on a time stressed, high stakes examination a valid assessment of a students' knowledge, skills or potential to perform effectively in any but this very peculiar and foreign environment ?

Conclusion

This research was conducted with the intention to examine learner authentication technologies and procedures and find examples that refute the "not possible" claim made by Moore and Kearsley almost twenty years ago. When the literature review was conducted to explore the relevant research regarding the issue of remote authentication of learners, several promising developments that indeed challenge the claim Moore and Kearsley made in 1996 stood out as a potential solution to this issue. These include biometric technologies and remote proctoring systems. This study confirms that secure learner authentication in distance education environment is possible. A combination of technology and administrative procedures may facilitate a secure testing environment. One may argue that it is not only the type of authentication that ensures academic integrity, but the degree to which it is standardized and consistently applied.

The main underlying issue when dealing with student authentication, is not with finding the right technology, but rather emerges as an imperative need to find a healthy compromise between credibility and accessibility of remote learning. Traditional authentication methods also make distance education more accessible, as access is open to anyone with a computer and Internet access. Credibility of distance education entails greater responsibilities for all the stakeholders. Therefore, putting greater emphasis on high level authentication strategies may require greater involvement of students, administrative and teaching staff in the evaluation process. A complete avoidance of secure testing is not reasonable. A system of checks and balances is what defines credibility. By minimizing over-reliance on measures that do not provide authorship and identity

validation, convenience and accessibility levels of distance courses may be affected. This may consequently change the face of distance education once again.

References

Anderson J. & Applebome P. (2011, December 1). Exam Cheating on Long Island Hardly a Secret. *The New York Times*. Retrieved from http://www.nytimes.com/2011/12/02/education/on-long-island-sat-cheating-was-hardly-a-secret.html?ref=satcollegeadmissiontest

Athabasca University. (n.d.). *Athabasca University : Canada's Leader in Online & Distance Education*. Retrieved December 11, 2011, from http://www.athabascau.ca

Bailie, J., & Jortberg, M. (2008). *A Collection of Papers on Self-Study and Institutional Improvement: Vol 3. Distance Learning Student Authentication: Verifying the Identity of Online Students.* Retrieved from http://www.franciscan.edu/home2/Content/dean/PAPERS/Inovation%20and%20change/3065.pdf

Bates, T. (2005). *Technology, e-learning and distance education* (2nd ed.). London: Routledge.

Bates, T., & Poole, G. (2003). *Effective teaching with technology in higher education: foundations for success*. San Francisco, CA: Jossey-Bass.

Baxter, P. & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report,8*(4), 544-559.

BioSig-ID (n.d.). *BioSig-ID | Biometric Signature ID (BSI) | Two-Factor Identity Verification | Multi-factor Authentication Security*. Retrieved February 2, 2012, from http://www.biosig-id.com

Biometric Signature ID. (November 5, 2009). *Identity Proofing for Student ID Verification Report of Pilot with University of Maryland University College*. Retrieved from http://www.biosig-id.com/wp-content/uploads/2011/07/Biometric-Signature-ID-and-UMUC-Case-Study.pdf

Branston, J. (2012, July 10). Former MCS Assistant Principal Indicted in Test-Taking Scheme. *Memphis Flyer*. Retrieved from http://www.memphisflyer.com/CityBeatBlog/archives/2012/07/10/former-mcs-assistant-principal-indicted-in-test-taking-scheme

Case, R, & Cabalka, P. (2009). Remote Proctoring: Results of a Pilot Program at Western Governors University. *Proceedings of the 25th Annual Conference on Distance Teaching and Learning,* Madison, WI. *Retrieved* on February 10, 2012 from http://www.uwex.edu/disted/conference/Resource_library/proceedings/09_19933.pdf

Chiesl, N. (2007). Pragmatic methods to reduce dishonesty in web-based courses. *Quarterly Review Of Distance Education*, *8*(3), 203-211.

The Open University. (n.d.). *Distance Learning Courses and Adult Education - The Open University*. Retrieved December 11, 2011, from http://www.open.ac.uk

eConcordia. (n.d.). *eConcordia*. Retrieved October 11, 2012, from http://www.econcordia.com

Eisenhardt, K. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, 14(4), 532-550.

Faculty Senate Committee on Technology (2005). *Kansas State University*. Retrieved October 1, 2012, from http://www.k-state.edu/facsen/policies/archives/ElectronicDevices1_05_000.pdf

Grijalva, T. C., Nowell, C., & Kerkvliet, J. (2006). Academic Honesty and Online Courses. *College Student Journal*, *40*(1), 180-185.

Higher Education Opportunity Act (2008) Higher Education Opportunity Act - 2008. U.S. *Department of Education.* Retrieved October 1, 2012, from http://www2.ed.gov/policy/highered/leg/hea08/index.html

Iqbal, F., Binsalleeh, H., Fung, B., & Debbabi, M. (2010). Mining writeprints from anonymous e-mails for forensic investigation. *Digital Investigation*, *7*(1-2), 56-64. Retrieved December 22, 2012, from the Science Direct database.

Isa, P., Samah, S., & Jusoff, K. (2008). Inculcating Values and Ethics in Higher Education e-Learning Drive: UiTM i-Learn User Policy. *Proceedings of World Academy of Science: Engineering & Technology*, *40*, 452-456. Retrieved March 1, 2012, from the Academic Search Complete database.

Kennedy, K., Nowak, S., Raghuraman, R., Thomas, J., & Davis, S. F. (2000). Academic dishonesty and distance learning: student and faculty views. *College Student Journal*, *34*(2), 309.

Kryterion. (n.d.). *Kryterion - Online Secure Testing*. Retrieved February 2, 2012, from http://www.kryteriononline.com

Levey, S., & Maynard, J. (January 17, 2011). Identity Proofing for Online Student ID Verification: Report of Pilot with Houston Community College. Retrieved from http://www.biosig-id.com/wp-content/uploads/2011/04/Biometric-Signature-ID-and-HCC-Case-Study-Final_0120111.pdf

McCabe, D. L., & Trevino, L. K. (1996). What we know about cheating in college: Longitudinal trends and recent developments. Change, 28(1), 28-33. (EJ 520 088)

McNabb, L., & Maynard, A. (2010). Software Only Biometrics to Authenticate Student ID Report of Pilot with the University of Texas System TeleCampus. Retrieved February 2, 2012, http://www.biosig-id.com/wp-content/uploads/2011/07/Biometric-Signature-ID-and-UT-Systems-pilot-results.pdf

Mitchell, R. (2009). Ethics in an online environment. *New Directions for Community Colleges*, (148), 63-70.

Moore, M. G., & Kearsley, G. (1996). *Distance education: a systems view*. Belmont: Wadsworth Pub. Co..

Morby, A. (2012, Jan 16). Skills card health and safety test cheats jailed. *Construction Enquirer*. Retrieved from http://www.constructionenquirer.com/2012/01/16/skills-card-health-and-safety-test-cheats-jailed

Mott, J. H. (2010). The Detection and Minimization of Cheating During Concurrent Online Assessments Using Statistical Methods. *Collegiate Aviation Review*, *28*(2), 32-46.

Neuman, W. L. (2006). *Social research methods: qualitative and quantitative approaches* (6th ed.). Boston: Pearson/ A&B.

Pansiri, J. (2005). Pragmatism: A methodological approach to researching strategic alliances in tourism. *Tourism and Hospitality: Planning & Development*, *2*(3), 191-206. Retrieved August 12, 2012, from http://www.cecc.com.au/clients/sob/research/docs/jpansiri/TourismandHospitalityPlanningandDevelopment.pdf

Pina, A. A. (2010). Online diploma mills: implications for legitimate distance education. *Distance Education*, 31(1), 121-126.

Penn State (n.d.). Penn State | Online Degrees, Online Courses, and Online Certificates offered by Penn State. *Penn State | Online Degrees, Online Courses, and Online Certificates offered by Penn State*. Retrieved October 5, 2012, from http://www.worldcampus.psu.edu

Powel, T. (2001) Competitive Advantage: Logical And Philosophical Considerations. *Strategic Management Journal*, 22: 875–888.

Scanlon, P. M. & Neumann, D. R. (2002) Internet plagiarism among college students. *Journal of College Student Development*, 43(3), 347-385.

School that gave MBA to cat sued. (2005). *Distance Education Report*, *9*(8), 7.

Sheridan, J., Alany, R., & Brake, D. (2005). Pharmacy students' views and experiences of Turnitin —an online tool for detecting academic dishonesty. *Pharmacy Education*, *5*(3/4), 241-250.

Smith, P. L., & Ragan, T. J. (2005). *Instructional design* (3rd ed.). Hoboken, N.J.: J. Wiley & Sons.

Software Secure. (n.d.). Secure Testing | Online Proctor | Software Secure. Retrieved February 3, 2013, from http://www.softwaresecure.com

Tuli, F. (2010) The Basis of Distinction Between Qualitative and Quantitative Research in Social Science: Reflection on Ontological, Epistemological and Methodological Perspectives. *Ethiopian Journal of Education and Sciences,* 6 (10), 97-108.

University of Maryland University College. (n.d.). *University of Maryland University College*. Retrieved February 3, 2011, from http://www.umuc.edu

Wikipedia (n.d.). List of animals with fraudulent diplomas. *Wikipedia, the free encyclopedia*. Retrieved December 22, 2012, from http://en.wikipedia.org/wiki/List_of_animals_with_fraudulent_diplomas

Zheng, R., Li, J., Chen, H., & Huang, Z. (2006). A framework for authorship identification of online messages: Writing-style features and classification techniques. *Journal of the American Society for Information Science and Technology*, *57*(3), 378-393.

Appendix A – Email Invitation

Personalized e-mail invitation to University staff inviting to participate in a study.

Dear <TITLE>. <NAME>,

My name is Alexander Amigud and I am a graduate student in the Master of Education in Distance Education program at Athabasca University. I am currently conducting research on identity control measures employed by universities to address possible identity fraud. Academic Identity Fraud is a form of cheating that involves deliberate impersonation of another individual in person or through the use of communication technology. My study will compare academic integrity policies and identity control strategies of the several leading distance education institutions, in three countries in order to examine the differences of institutional level identity control strategies, their effectiveness and challenges as well as identify barriers to their implementation from the perspective of university administrative staff. Your perception of the effectiveness of these measures will also be examined. This study is comprised of two components, a five-scale Likert-like questionnaire administered via e-mail or online and a follow up phone interview.

After the survey data has been analyzed a short follow up phone interview may be conducted to verify or clarify survey information or ask additional questions. The phone interview should not exceed 15 minutes. It will be recorded with your permission. Your name will be removed from the transcript to ensure privacy. All data will be securely stored and password protected and deleted upon project completion.

Please note that participation in this study is voluntary. You are invited to participate and may withdraw from the study at any time. If at any time you

decide to withdraw, your data will not be used and deleted immediately. This study calls for a new organizational strategy to address academic misconduct and identity control measures such that minimize opportunities for identity fraud in an online environment. Strategy recommendations will be made following the analysis. We will share an electronic copy of the final thesis report with all participants. We trust this document will be useful to you in developing your own academic misconduct policies. Your participation will be very important in an effort to reinforce credibility of distance education. Please fill in the following consent form and return to <EMAIL>.

[ ] I consent to participate in this study. Name _____ Date_____
[ ] I refuse to participate in this study.

If you have any questions, please do not hesitate to contact me.

Appendix B - Questionnaire

1. Identity fraud has emerged as an issue at my institution.

[ ] Strongly Agree [ ] Agree [ ] Neither agree nor disagree [ ] Disagree [ ] Strongly Disagree Please add a brief comment to explain your answer:

2. My institution tracks and trends academic misconduct data.

[ ] Strongly Agree [ ] Agree [ ] Neither agree nor disagree [ ] Disagree [ ] Strongly Disagree Please add a brief comment to explain your answer:

3. My institution has an adequate system of identifying online students before each project or paper submission.

[ ] Strongly Agree [ ] Agree [ ] Neither agree nor disagree [ ] Disagree [ ] Strongly Disagree Please add a brief comment to explain your answer:

4. My institution has an adequate system of identifying online students before each final and/or midterm exams.

[ ] Strongly Agree [ ] Agree [ ] Neither agree nor disagree [ ] Disagree [ ] Strongly Disagree Please add a brief comment to explain your answer:

5. My institution has encountered barriers to implementation of identity control measures.

[ ] Strongly Agree [ ] Agree [ ] Neither agree nor disagree [ ] Disagree [ ] Strongly Disagree Please add a brief comment to explain your answer:

6. The identity control measures my institution employs to authenticate the identities of online students are effective.

[ ] Strongly Agree [ ] Agree [ ] Neither agree nor disagree [ ] Disagree [ ] Strongly Disagree Please add a brief comment to explain your answer:

7. The system my institution employs to conduct remote identification of test takers has challenges.

[ ] Strongly Agree [ ] Agree [ ] Neither agree nor disagree [ ] Disagree [ ] Strongly Disagree Please add a brief comment to explain your answer:

8. The best practice for authenticating the work of remote learners is:

[ ] Remote Proctoring using web cams [ ] Biometric Authentication asserting the identity of the student by fingerprints, keyboard activities etc.[ ] Traditional Proctoring [ ] Policy Enforcement [ ] Other

Please add a brief comment to explain your answer:

Appendix C - Research Ethics Review Committee Approval

MEMORANDUM

DATE: June 27, 2012

TO: Alexander Amigud

COPY: Dr. Terry Anderson (Research Supervisor)
Janice Green, Secretary, Athabasca University Research Ethics Board
Dr. Simon Nuttgens, Chair, Athabasca University Research Ethics Board

FROM: Dr. Rick Kenny, Chair, CDE Research Ethics Review Committee

SUBJECT: **Ethics Proposal #CDE-12-07: *"Analysis of Institutional Level Identity Control Strategies in Distance Education Environment: A Survey of Administrative Staff"***

The Centre for Distance Education (CDE) Research Ethics Review Committee, acting under authority of the Athabasca University Research Ethics Board to provide a process of review for minimal risk student researcher projects, reviewed the above-noted proposal and supporting documentation.

I am pleased to advise that the above-noted research has been **APPROVED TO PROCEED.**

This approval of your application will be reported to the Athabasca University Research Ethics Board (REB) at their next monthly meeting. The REB retains the right to request further information, or to revoke approval at any time.

The **approval for the study** "as presented" **is valid for a period of one year from the date of this memo**. If required, an extension must be sought in writing prior to the expiry of the existing approval. **A Final Report is to be submitted** when the research project is completed. The reporting form can be found online at http://www.athabascau.ca/research/ethics/ .

As implementation of the proposal progresses, if you need to make any significant changes or modifications prior to receipt of a final approval memo from the AU Research Ethics Board, please forward this information immediately to the CDE Research Ethics Review Committee via rebsec@athabascau.ca, for further review.

If you have any questions, please do not hesitate to contact Janice Green at rebsec@athabascau.ca

Centre for Distance Education Research Ethics Review Committee
(A Sub-Committee of the Athabasca University Research Ethics Board)
1 Athabasca Drive, Athabasca, AB, Canada T9S 3A3
e-mail: janiceg@athabascau.ca
Telephone: (780) 675-6718
Fax: (780) 675-6722