Direct Lending Fraud:
One University's Response to Identity Fraud in Online Learning

Vickie Fredrick
Webster University
470 E Lockwood Ave, LH212
Saint Louis, Missouri 63119
(314)968-5911
fredrivl@webster.edu

ABSTRACT

In Fall 1997, an individual named Talmadge Travis Graham was admitted and registered at Webster University using the stolen identity of four unsuspecting individuals. He also applied and was granted Stafford loans under two of the four identities. Mr. Graham had been a Webster University graduate student during the previous academic year, never completing a course, but successfully learning how Webster University processed Stafford Loans and disbursed the credit balances. His fraud was discovered by accident. He paid the application fee of multiple students using a stolen checkbook with checks on an account that had closed. Collections personnel became suspicious of multiple bounced checks on multiple student accounts with the name on the account that did not match any of the student account names. His other error was to apply under all identities using one of two addresses. These two factors resulted in the detection of the fraud. The University promptly informed the Department of Education and the FBI set up a sting operation on Webster University's main campus to arrest Talmadge Travis Graham.

Times have changed. Students apply and complete the FASFA form now online. Courses are delivered online. Finally, refunds of credit balances are also delivered electronically. In the new electronic age, the individuals behind identity theft are *faceless*. However, certain facts remain unchanged. The pool of available money to steal is considerable, the fraudsters have seen first hand how easy it is to steal, and the Department of Education and the resources available to the administrative offices of Universities have not kept pace with technology.[i]

Within the past three years, Webster has identified and reported 3 identity theft abuses involving multiple student accounts. This paper details the lessons learned and steps taken by Webster University to proactively identify Straw Students. The process remains fluid as those attempting to defraud the University continue to learn and adapt to the preventive measures that we have installed.

INTRODUCTION

Webster University, founded in 1915 with its home campus based in Saint Louis, Missouri, is the only tier 1, private, nonprofit university with campus locations around the world including metropolitan, military, online and corporate, as well as, American-style traditional campuses in North America, Europe and Asia. Webster University educates more than 25,000 undergraduate and graduate students globally, and has been a recognized leader in both international and military education for more than 30 years. Our mission is to ensure high-quality learning experiences that transform students for global citizenship and individual excellence.

Webster's graduate online programs have expanded from infancy in 1999 to more than 62,000 credit hours annually in fiscal year 2011-12. Nine thousand unique Webster students took at least one online class last year. One out of every four of Webster University graduate student enrollments was online. Our online students are from 49 states and 63 international locations. In 2011-12, the University awarded and processed over $187 million under the Federal Direct Loan program.

INITIATIVE STATEMENT

The University has been targeted by both "Pell Runners" and "Straw Student Rings". This paper discusses Webster University's interdivisional approach to proactively respond and identify "Straw Student Rings". For those that are unfamiliar with the term, straw student rings are a mix of suspecting and/or unsuspecting students that are recruited or have their identity stolen by a ringleader or kingpin. When recruited, the willing accomplice knowingly enrolls,

obtains financial aid and drops out. These students receive a cut of the financial aid disbursed. In the latter, the unsuspected student is an unwitting victim whose stolen identity is used to defraud both the University and the Department of Education.[ii]

ESTABLISHING A PROCESS TO EARLY DETECT ONLINE STRAW STUDENT FRAUD

(Design & Implementation)

In the past three years, Webster University has identified and referred 3 online straw student fraud schemes, involving 51 individuals, to the Office of Inspector General. This pales in comparison to the 886 fraud schemes, comprised of 17,600 individuals, reported by the University of Phoenix.[iii] However, every instance of this fraud presents reputation and financial risk to the University.

Phase I – First Fraud

As is understandable, our design and implementation of the process to identified suspect straw student fraud has been reactionary. The first fraud, discovered in 2009, was identified *after* the ringleader had successfully processed straw students through our system for four terms. The ringleader got greedy and enrolled 14 new graduate straw students in our online programs for the Fall I term. All had one of two South Carolina addresses, and all but one had received Stafford loan proceeds. Data mining identified 9 additional online straw student graduate enrollments that spread over the Spring I, Spring II and Summer 2009 terms. Our research also identified the ringleader, Michelle Owens. Michelle, a previous Webster University graduate online student and “Pell Runner”, pleaded guilty to one count of federal

student financial aid fraud and one felony count of mail fraud on June 8, 2011. Approximately $125,000 of Federal funds were disbursed and lost.

The lessons learned from the first fraud were as follows:

- These criminals require one or more controlled physical address(es). Webster University utilizes HigherOne to distribute refunds of student account credit balances. In order to sign up for refund distributions, students must receive the HigherOne mailing in order to complete an electronic logon, authentication, and registration. One early warning sign of a Straw Student Ring is identifying multiple students with the same physical address.
- Typically, these criminals only logon to the online class to introduce themselves. Their overall time spend in the online class is minimal. They do not complete any assignments or quizzes.
- The straw students typically do not meet the basic eligibility requirements, i.e., possesses a bachelor degree, but the criminal falsely indicated on the enrollment application that they did. The University practice's was to provisionally admit students and provide a one term grace period for the student to provide an official transcript of his/her degree. Disbursement of financial aid policies followed this rule as well.

The University's response was as follows:

- Initiate a University policy that no graduate financial aid disbursement would be released until an official transcript of a conferred bachelor degree was received by the University. However an exception basis, the University would release graduate financial aid disbursements if the student was able to provide a copy of a state issued id or U.S. passport.

- Institute “Red Flag” training program to sensitize employees of designated departments to identify and report suspicious student events or observations.

Phase 2 – Second Fraud

The second fraud, discovered in April 2012, was identified in the middle of the fraud. Approximately, $55,000 of federal funds were disbursed and lost.

The lessons learned from the second fraud were as follows:

- Criminals are reactive and creative. They adapted to our change in processes by obtaining copies of state issued id’s in the names of the straw students.
- Criminals are anxious to get paid as quickly as possible, and will place multiple calls to admissions, financial aid, bursar, and online learning offices requesting reimbursement.
- Criminals get lazy and make errors. They logon for multiple students using the same ip addresses, within minutes of completing the last. Also, in this case, they structure the straw student email addresses with similar characteristics, but don’t necessarily set up the address prior to providing it to the University. In this instance, one of those email addresses was already in use. When our automatic response email was issued, the original holder of the email address contacted the University.
- The Inspector General’s Office of the Department of Education does not have the resources to investigate and pursue prosecution unless the amount of loss exceeds an unnamed threshold, even when provided the name and information of the suspect ringleader.

The University's response was a follows:

- Establish a task force with members representing internal audit, finance, bursar and student enrollment. Once suspect activity is detected each member is tasked to initiate searches of paper and database records, on-line course activity and logons and e-records for details to identity suspect Straw Students. All information is gathered and maintained centrally by Internal Audit. The group is tasked to take appropriate action to minimize the risk to the University, to report to administration and the audit committee, and to report, as appropriate, to the Inspector General's Office of the Department of Education.
- Immediately stop the exception granting release of graduate financial aid disbursements if the student was able to provide a copy of a state issued id or U.S. passport. In addition, the official transcript requirement (high school transcript or GED) was implemented for the undergraduate program.
- Re-train and/or prioritize "red flag" training for an expanded employee population.

<u>Phase 3 – Third Fraud</u>

The third fraud, discovered in October 2012, was identified prior to any credit balance disbursement of Federal funds.

The lessons learned from the third fraud were as follows:

- Criminals continue to be reactive and creative. They were again able to adapt to our change in process. This time the ring leader used the stolen identities and information to:
  - Obtain Federal aid,

- Official transcripts of conferred graduate degrees from unsuspecting colleges and universities, and
- Gain enrollment into a Webster University online course.

- People provide too much personal information in social media. We were able to find information on every straw student (i.e., college attended, degree conferred, etc.) on social media sites, such as Face Book and Linked In. One defrauded student admitted that his social security number, personal and education information were printed on his CV which was available on the web.
- Criminals still require a controlled physical address, but try to mask this by changing the addresses of the students once the HigherOne card has been issued.
- Criminals continue to be lazy.
  - They logon for multiple students using the same ip addresses, within minutes of completing the last.
  - They structure the straw student email addresses with similar characteristics.
  - They provide the same phone number for multiple straw students.
  - They only logon to the online class to introduce themselves, many times only altering their introduction script to change the name.
  - Their overall time spend in the online class is minimal. They do not complete any assignments or quizzes.
- Due to limited resources, the Inspector General's Office of the ED will not take any action if the fraud is identified and prevented without loss.

The University's response was as follows:

- Hire an external consultant to review our internal processes and make recommendations for improvements. Our response to these recommendations are closely monitored by administration and reviewed with the audit committee.
- Examine internal processes and requirements relating to the release of student official transcripts from our Registrar's Office. Ensure that requests for transcripts are authenticated prior to release.
- The University reached out to its disbursing agent, HigherOne, and asked what if any programs they had in place or were developing to deal with identity fraud. HigherOne has introduced a new partner, iDatafy, that appears to have an outstanding understanding of the issues and product to move us into that needed electronic early warning, proactive role. We will be exploring this product in the near future.
- Form an interdivisional Think Tank group to review the lessons learned, actions taken and recommendations for improvement to establish a systematic, proactive and preventive process to early detect and prevent Straw Student Ring fraud. Think Tank members represent the divisions of Finance, Student Enrollment Services and Academic Affairs and include the offices of Treasury, Bursar, Financial Aid, Admissions, Online Learning Center, Registrar, Internal Audit, Accounting, Information Services, Public Safety, and Risk Management.

The initiative and the steps taken to date did not require additional personnel or capital equipment. It did require programming staff prioritization. In addition, it relied on the data mining and reporting writing strengths of certain employees within the University. Finally, the cost of an external consultant review was managed under the budget of internal audit. Much of the time and effort expended by numerous employees has been under the guise of other duties as required.

BENEFITS

As is portrayed in the VISA commercials, the benefit we have received from this initiative is “priceless”. Every instance of this fraud has some financial risk, but it is almost impossible to place a value on the averted risk to the University’s reputation.

The original fraud in 1997 and the first straw student ring fraud in 2009 were discovered by the University. The University helped the Department of Education to successfully prosecute the perpetrators. However, when the news hit the media, I was asked countless times by my friends, “What kind of fraud is going on at the University?” In summary, there is no “reputation value” in uncovering and helping to prosecute a criminal. The general public only “hears” the part of the story that says this fraud or criminal action happened at Webster University.

In addition, even though the Think Tank has had only one meeting. The ideas and sharing of information that occurred at that meeting were invaluable. Within two hours, individuals that previously only played a part of the production, could then see the

whole picture, and were already thinking about ways that we could improve on what we are already doing.

RETROSPECT

In retrospect, I only wish we could have reacted faster and anticipated better. However, I believe we are on our way to making notable improvements to our processes within the next six months.

---

[i] 11/14/2012, Dave Wengel, "A Proactive Stand Against Financial Aid Fraud Whitepaper," http://www.prweb.com/releases/2012/11/prweb10128418.htm

[ii] Ibid.

[iii] 5/23/12, Transcription of Negotiated Rulemaking Sessions and Public Hearings 2012, U.S. Department of Education (ED) Office of Post Secondary Education, Pages 20-12, http://ww2ed.gov/policy/highered/reg/hearulemaking/2012/transcript-phoenix052312.pdf