



IT'S A
JUNGLE
OUT THERE

FALL 2014 CONFERENCE

MISSOURI ASSOCIATION OF STUDENT FINANCIAL AID PERSONNEL

**Designing a Proactive Financial Aid
Fraud Protection Program**

Vickie Fredrick
AVP and Asst. Treasurer

Financial Aid Fraud is Here – and Here To Stay



How Can Online Financial Aid Fraud Occur?



Webster University

- With campuses on 4 continents, Webster University educates more than 25,000 students annually
 - ✓ > 60,000 credit hours or 1,700 online courses per year
 - ✓ 1 out of every 4 graduate student enrollments are online
 - ✓ Successfully identified and referred “Straw Student Ring Schemes” to the Office of the Inspector General
- Case Study # 1



The Women's Maximum Security Correctional Facility in Greenwood South Carolina



- ✓ 23 applications/enrollments over a one year period
- ✓ 3 physical addresses
- ✓ Seeking loans of \$467,500, \$194,900 received and processed



Fraudsters Are Creative

- Case Study #2
- Summary
 - ✓ 26 applications/enrollments over a 8 month period
 - ✓ 3 physical addresses
 - ✓ \$118,600 received, but only \$55,600 refunded and lost
 - ✓ Identified name and phone number of suspect
 - ✓ Inspector General's Office of ED was provided information and documents, but responded that prosecution was unlikely due to low \$'s lost.



Lessons Learned



Be Proactive



- Train employees to identify and report suspicious student events or activities (“Red Flags”)
- Communicate
- Establish multi-departmental task force



Possible Preventative Controls

- Common identifying data
- Increase verification efforts
- Enhance new student orientation and registration requirements
- Timing of student loan disbursements and refunds
- Loan/attendance history



Red Flags & Detection

- Student Red Flags:
 - Overly aggressive pursuit of refund
 - Low or minimal class participation
 - Payment address or bank account/routing number
 - Phone #
 - Logon IP address
- Train and empower employees when they feel threatened



Prevention Must be a Priority

- Case Study #3
- How the fraudsters adapted:
 - ✓ Started with multiple state addresses, then quickly changed to one of five
 - ✓ Not only involved identity theft, but fraudster defrauded other Universities into releasing official transcripts
 - ✓ They logon to course, but did not participate, except to introduce, in order to show time in course
- Your prevention controls must anticipate and adapt.



What is at Stake?

- Reputation Risk
- Financial Risk
- Academic Cost/Risk



Key Steps that You Can Take

- Train and empower your staff to identify and report red flags
- Establish cross functional task force and communications
- Develop tools to identify Common Data Across Student Enrollments
- Subscribe to iDatafy's free "Hot Addresses" file
- Utilize Predictive Analytical Software, such as Analyst/X Office distributed by Advizor Solutions.



Summary

- Fraud will occur
- Be proactive
- Collaborate and communicate
- Adapt & stay ahead of the fraudsters
- Make this a priority



Credits

- HigherOne's Alert! Fraud Service
- iDatafy.com for HotAddress™ by iDatafy®
- Advizorsolutions.com for Analyst/X Office

Vickie Fredrick, fredrivl@Webster.edu, 314-968-5911

