Designing a Proactive Financial Aid Fraud Protection Program

Vickie Fredrick
AVP and Asst. Treasurer
Webster University
October 5th, 2015

Today's Objectives

- Identify online fraud "Red Flags"
- Financial aid fraud risk factors
- Reactive steps
- Next steps to develop a financial aid fraud prevention plan

Epilogue:
Financial Aid Fraud is Here – and Here To Stay

The Fraud Triangle

- **Motivation** or pressure to commit the fraud
- **Opportunity** to commit the fraud without significant threat of discovery
- **Rationale** for commission of the fraud that overrides the sense of right and wrong

How Can Online Financial Aid Fraud Occur?

Identity Theft

- 533 data breaches
- > 140 million personal records exposed
  - September 1st report from the Identity Theft Resource Center (ITRC)

8.4% of the data breaches and .5% of the records exposed were in the educational sector

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

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

- 23 Applications/enrollments over one year
- 3 physical addresses
- Seeking loans of $465,500, but only $194,900 processed

Case Study Points

- Red Flags
  - ✓ Multiple students with same address,
  - ✓ All new graduate students,
  - ✓ All taking online classes
- Financial aid risk factors
  - ✓ Tuition Dependent, Enrollment Driven
  - ✓ Streamlined application and enrollment processes
- Reactive steps
  - ✓ Hired an Independent Investigator
  - ✓ Turned the information over to the ED's Inspector General
  - ✓ External communications from Inspector General and independent auditors forced a policy change

Lessons Learned

- Fraudsters learn your system and adapt
- If you have an exception, they will find it.
- If you close that exception, they find another way.
- Don’t fall asleep -- Fraudsters are creative

How Fraudsters Adapt

- Case Study #2 Details
  - ✓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.

Case Study Points

- New “Red Flags”
  - ✓ Address on student’s submitted identification DID NOT agree to the address on the student’s record
  - ✓ Criminal was anxious to receive refund as quickly as possible and made multiple phone calls to various departments within Webster. Name on caller id DID NOT agree to the name on the student account
- Financial aid risk factors
  - ✓ Increasing pressure to maintain enrollments
  - ✓ Increasing focus on customer service and “do what it takes to make the customer happy”
  - ✓ Tendency to identify a reason or explanation for why not a “Red Flag”
- Reactive step
  - ✓ Eliminate the exception; require official transcripts prior to requesting loan funds from the ED

How Fraudsters Adapt

- Case Study #3:
  - ✓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
  - ✓Students logged in to course, but did not participate, except to introduce, in order to show time in course
- Focus on **Prevention**

Student Red Flags

- Overly aggressive pursuit of refund
- Low or minimal class participation
- Payment address or bank account/routing number
- Phone #
- Logon IP address
- Official Transcript

Financial Aid Fraud Risk Factors

- Tuition dependent; enrollment driven
- Streamlined application and enrollment
- Exception based processes
- Department and process silos
- Rationalization of data
- Customer service

Reactive Steps To Being Proactive

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

Preventative Controls

- Common identifying data
  - ✓ iDatafy's free "Hot Addresses" file
  - ✓ Alert! Fraud Protection
  - ✓ Predictive Analytical Software
- Increase verification efforts
- Timing of student loan disbursements and refunds
- Loan/attendance history

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