



FLEMING

Fraud Prevention Training
- Expense Management and
Vendor Payments

Presented by : Finance

Agenda

- Training Objectives
- Fraud Triangle
- Case Studies
- Fraud Types
 - Expense Reimbursement
 - Vendor Payments
 - International Student Payments
- The Next Normal : Preparing for a Post-pandemic Fraud Landscape
- Building an Anti-Fraud Environment
- Questions



Objectives

Understand the fraud triangle to anticipate and address situations that could lead to fraud

Explain the impact and significance of fraud and its effect on organizations through review of case studies

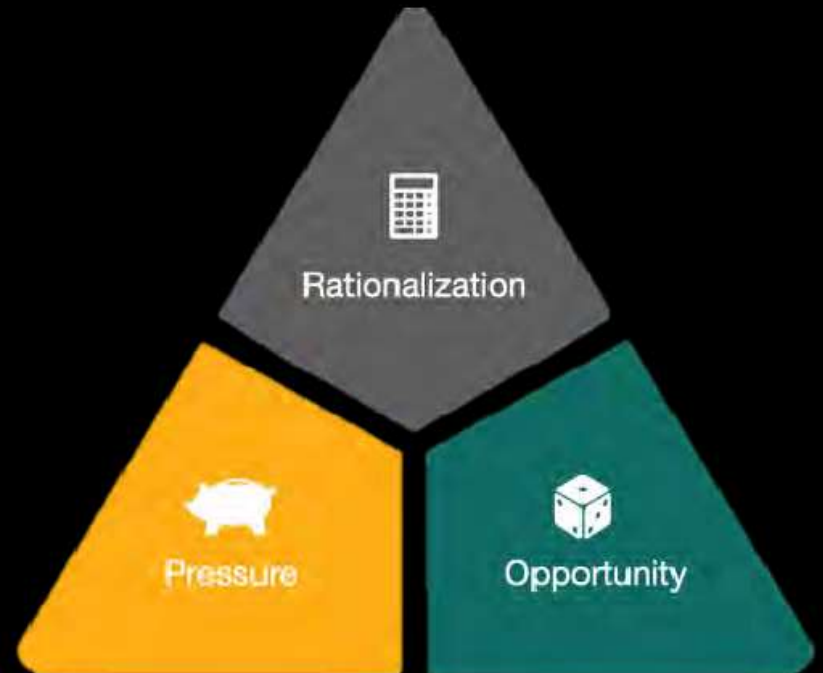
Identify 'red flags' that signal possible fraudulent practices

Remind staff of the reporting mechanisms for fraud, including the whistleblower line



Fraud Triangle

- Why do people commit Fraud?
- Click video



Case #1 – In Higher Education

- Organization: Vassar College (New York)
- Type of fraud: Vendor payment fraud
- What happened: Project manager set up a fictitious construction company and made payments for a fake construction project, totaling \$1.9M
- How was the fraud identified: Fraud identified through manager review
- Outcome: The project manager and his wife were charged with first-degree larceny, which included 4-12 months in jail and 5 years' probation. The couple also had to repay the money. The organization had reputation loss and had to complete a full revision of their financial policies.



Case #2 – Close to Home

- Organization: Peterborough Big Brothers Big Sisters
- Type of fraud: Payment fraud
- What happened: Executive director opened a bank account and used forged documents and over a nearly decade-long period, funneled almost \$120,000.
- How was the fraud identified: Fraud identified through analytics (review of “abnormalities” by Board)
- Outcome: Executive director was sentenced to two years less a day in custody, with at least one year of that under house arrest. The penalty was considered “light” and only provided as she paid substantial restitution and donation (repayment of \$107,016.94 and a \$19,000 donation). The organization itself had financial loss in the form of the direct loss of resources to the executive director, indirect financial loss due to loss of donor support and some funding sources, as well as indirect reputation loss.

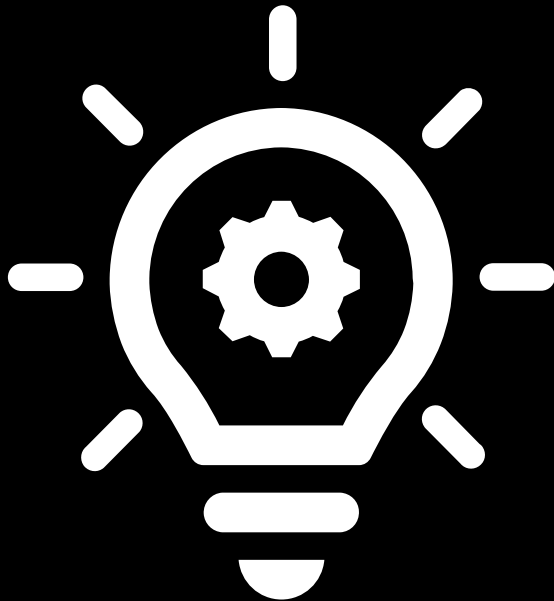


Types of Fraud for Discussion

- Expense Reimbursements
- Vendor Payments
- International Student Payments



Expense Reimbursements



Fun fact:

According to the Certified Fraud Examiners' 2018 Report to the Nations, expense reimbursement fraud accounts for **21%** of fraud in small businesses and **11%** of fraud in large businesses.

Expense Reimbursements

Common categories of expense reimbursement schemes:

1. Mischaracterized expenses
2. Fictitious expenses
3. Overstated expenses
4. Multiple reimbursements



Expense Reimbursements

Mischaracterized expenses

Personal expenses passed off as a business related expense.

Examples:

- “Office” related purchases incurred while working from home



Expense Reimbursements

Fictitious Expenses

Fake receipts.

Examples:

- Invoice from a fake supplier
- Real supplier invoice digitally modified

Expense Reimbursements

Overstated Expense Reimbursements:

Legitimate expenses that are inflated.

Examples:

- Overstating mileage distances
- Altering receipts to show larger amounts paid
- Returning a higher price item for a less expense alternative



Expense Reimbursements

Multiple Expense Reimbursements:

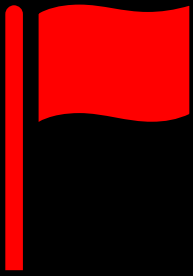
Submitting expense claim for same item multiple times.

Examples:

- Submitting same receipt multiple times
- Submitting travel reimbursement when coworker drove
- Submitting meal receipt when away at conference but meal is provided



Expense Reimbursements



Red flags:

- Unusual dates and times
- Unusual amounts
- Expense claims lacking information
- 'Gut feel'

Expense Reimbursements

Controls and processes to prevent expense reimbursement fraud:

1. Maintain a travel reimbursement policy/operating procedure
2. Require detailed receipts (preferably originals), including documentation of business purpose
3. Require second review (i.e. direct supervisor and AP)
4. Review data analytics / technology use (Evolve module)
5. Trust, but verify



Vendor Payments

Common categories of vendor fraud schemes:

1. False payments
2. Check alterations
3. EFT alterations
4. Over-billing



Vendor Payments

False Payments:

Payment is made but no goods/services rendered.

Examples:

- Payment made to an employee through a fake vendor.
- Payment made for services not received by the College.

Vendor Payments

Cheque alterations:

Information on the cheque is altered to defraud someone.

Examples:

- Adjusting cheque amount
- Adjusting cheque payee
- Adjusting cheque date

Vendor Payments

EFT alterations:

Vendor banking information is falsely updated by a fraudster.

Examples:

- Adjusting bank account number

Vendor Payments

Over billing:

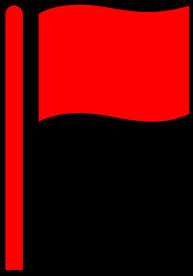
Purposely overcharging in price/quantity.

Examples:

- Billing for units not received
- Charging a unit price greater than contract/PO stated



Vendor Payments



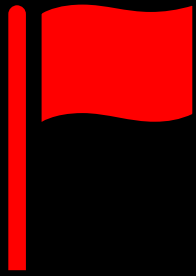
Red flags:

- Vendors with similar names
- Rounded dollar amounts
- Incomplete documentation
- Duplicate payments to the same vendor
- Vendor's prices that seem unusually low or high
- Repeated purchases from a vendor with a record of poor quality goods or services
- Tips or complaints from employees, customers or vendors



FLEMING

Vendor Payments



Red flags:

- Vendors that seem unusual or are unapproved
- Payments that consistently fall just under the amount requiring authorization
- Invoices in sequence
- Invoices that look unprofessional or photocopied
- Invoices that are missing key details, such as address and phone number
- A vendor's email address that uses a free provider, such as Gmail
- Vendor address that look to be residential addresses



Vendor Payments

Controls and processes to prevent vendor fraud schemes:

1. Vendor database management
2. Use of Purchase Orders
3. Multi step approvals
4. Segregation of duties



International Student Payments

Common categories of international student payment fraud schemes:

1. Third Party Interceptions
2. Tuition Payments Using Stolen Credit Cards




International Student Payments

Third Party Interceptions:

Parties overseas misrepresenting themselves as official agents or official agents intercepting tuition fees on the pretense of paying them on behalf of students

Examples:

- Official representative fraudulently taking the students' tuition fees and not paying them to the College
- False agent acting as a College representative and taking the students' tuition fees and not paying them to the  **FLEMING** College

International Student Payments

Tuition Fee Payment Using Stolen Credit Cards:

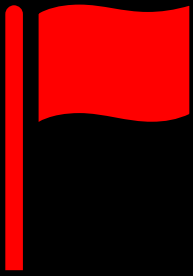
Students pay a discounted fee to an intermediary and the intermediary uses a stolen credit card to create payment. While many of the credit card charges are unsuccessful, some are successful and then later charged back to the institution.

Examples:

- Student pays intermediary \$5K to settle \$10K tuition bill. The intermediary uses stolen credit cards to pay the College. The payments appear successful and then one week later, Fleming receives a “chargeback”, i.e. payment pulled back by the bank.



International Student Payments



Red flags:

- CIBC (our portal for International student payments) indicates they have blocked a transaction.

International Student Payments

Controls and processes to prevent international student fraud schemes:

1. CIBC international student built in controls (e.g. blocking the student ID from further transactions)
2. Clear processes for tuition payments documented on student communications/website
3. Thorough review of official agent representatives to ensure they are trusted



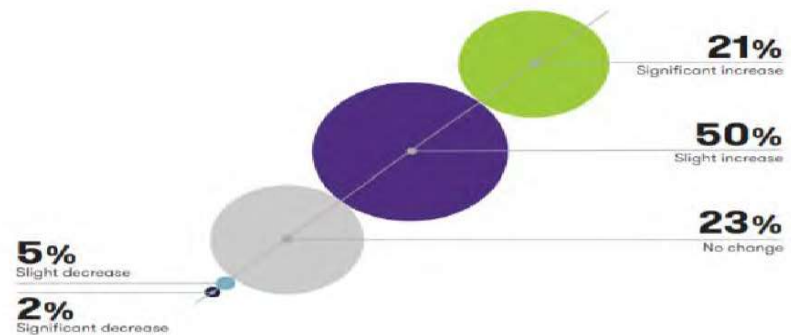
The Next Normal : Preparing for a Post-Pandemic Fraud Landscape

Change in the amount of fraud uncovered



51% of organizations have **uncovered more fraud** since the onset of the pandemic

Expected change in the overall level of fraud impacting organizations



71% expect the **level of fraud** impacting their organizations to **increase** over the next year

Build an anti-fraud control environment : Improve employee awareness in Fraud

1

Update/conduct
internal fraud
awareness training

2

Update/conduct a
fraud risk
assessment

3

Make operational
changes to the fraud
risk management
program

4

Update/create a
Enterprise risk map
or risk register

5

Conduct/expand due
diligence for third
and or fourth party
relationships



FLEMING

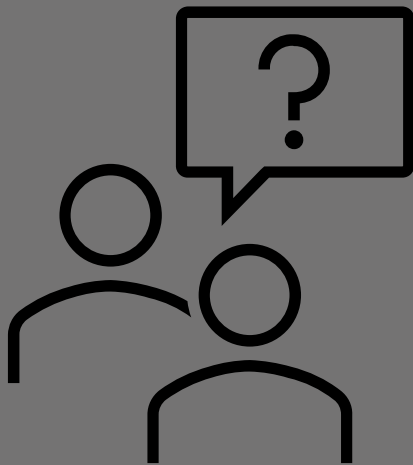
Reminder

- We have a Whistleblower Policy
- Complaints can be made in a variety of methods:
 - By mail
 - In person
 - By phone
 - By email:

Whistleblowing@flemingcollege.ca



Questions



If you have further questions, please
contact :
[vpcorporatefinance@flemingcollege](mailto:vpcorporatefinance@flemingcollege.ca)
[.ca](mailto:vpcorporatefinance@flemingcollege.ca)

Thank you

