Governor's Office of Crime Prevention and Policy (GOCPP)

Grants Fraud (Risks and Prevention) – Module 2 (Common Fraud Schemes)

Thursday, September 18, 2025

OFFICE OF THE GOVERNOR
Wes Moore

Maryland
GOVERNOR'S OFFICE OF CRIME PREVENTION AND POLICY

https://gocpp.maryland.gov/

This presentation is intended for general education and/or informational purposes only and does not replace specific and independent professional advice nor constitutes legal guidance. Material contained herein developed based on information available as of July 1, 2025.

General Housekeeping

- Videos of previous training session as well as the slides from this session will be available at https://gocpp.Maryland.gov/grants/.
- In order to receive a Certificate of Completion, all participants must complete the pre-training assessment (https://s.zoom.us/m/b9D6kT7ZS) and the post-training assessment (https://s.zoom.us/m/b9Ea1znbc). You can also access the assessments using the QR codes below:

Pre-Training Assessment

Post-Training Assessment

Maryland
GOVERNOR'S OFFICE OF CRIME PREVENTION AND POLICY

Common Fraud Schemes

Module 2

Learning Objectives

- **Explain** the mechanics of prevalent fraud schemes in grants management.
- **Illustrate** these schemes with real-world case studies to deepen understanding.
- **Develop** the ability to recognize how these schemes manifest in practical scenarios.
- **Prepare** to identify potentially fraudulent activities by understanding their common patterns.

Introduction to Fraud Schemes: How Perpetrators Execute Fraud

- Fraud isn't just an idea; it's a planned, executed deception, and schemes are the specific methods fraudsters use.
- **Key Idea:** Fraud isn't just an idea; it's a planned, executed deception. Schemes are the specific methods fraudsters use.
- **Why Study Them?**
  - To anticipate where and how fraud might occur.
  - To implement targeted controls.
  - To aid in detection and investigation.
- **Analogy:** If red flags are symptoms, fraud schemes are the underlying diseases.

Categorization of Schemes: A Framework

- We'll begin by outlining the common categories of fraud schemes in grants management.
- **Introduction:** We'll explore schemes often grouped by *how* they're carried out or *what* they target.
- **Common Categories (For this module):**
  - **Asset Misappropriation:** Theft of cash or noncash assets.
  - **Financial Statement Fraud:** Falsifying records.
  - **Corruption:** Bribery, kickbacks, or conflicts of interest.
- **Focus for Grants:** While all apply, we'll emphasize those most common in grants, often blending categories.



Ghost Employees/Vendors: The Invisible Payee

- Ghost employees/vendors are situations that involve creating fictitious employees or vendors on payroll or vendor lists to divert funds.
- **How It Works (Employees):**
  - Adding fake names to payroll.
  - Keeping terminated employees on payroll.
  - Creating fake timesheets/records for nonexistent work.
- **How It Works (Vendors):**
  - Setting up fake vendor companies.
  - Colluding with existing vendors to submit inflated or fake invoices for nonexistent services/goods.
- **Impact:** Direct loss of grant funds, inflated project costs.



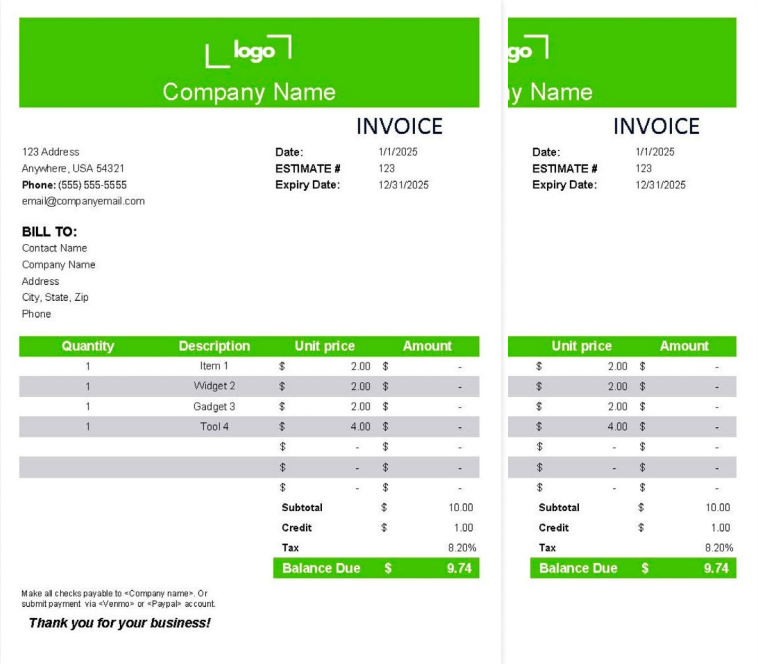
False Billing/Invoicing: The Inflated Charge

- False billing occurs when invoices are submitted for goods or services that were never provided, or for inflated quantities or prices.
- **Common Tactics:**
  - Billing for "phantom" services (e.g., consultants who never worked).
  - Inflating the hours worked by staff or contractors.
  - Charging for more expensive materials than actually used.
  - Billing for items not delivered or in lesser quantities.
- **Often Involves:** Collusion between an employee and an external vendor.
- **Impact:** Wasted grant funds, overpayment for services.



Duplicate Billing: Double Dipping

- This scheme involves submitting the same invoice or expense multiple times for payment.
- **How It Occurs:**
  - Submitting original and then a copy of the same invoice.
  - Submitting invoice to different grants or departments.
  - Changing slight details (date, invoice number) to appear unique.
  - Claiming the same travel expenses on different reports.
- **Red Flags:** Identical invoice amounts, vendor names, or item descriptions across multiple payments.
- **Impact:** Direct loss of grant funds through overpayment.



logo

Company Name

INVOICE

123 Address
Anywhere, USA 54321
Phone: (555) 555-5555
email@companyemail.com

Date: 1/1/2025
ESTIMATE # 123
Expiry Date: 12/31/2025

BILL TO:
Contact Name
Company Name
Address
City, State, Zip
Phone

Quantity	Description	Unit price	Amount
1	Item 1	$ 2.00	$ -
1	Widget 2	$ 2.00	$ -
1	Gadget 3	$ 2.00	$ -
1	Tool 4	$ 4.00	$ -
		$ -	$ -
		$ -	$ -
		$ -	$ -
		Subtotal	$ 10.00
		Credit	$ 1.00
		Tax	8.20%
		Balance Due	$ 9.74

Make all checks payable to <Company name>. Or submit payment via <Venmo> or <Paypal> account.

Thank you for your business!

go
y Name
INVOICE
Date: 1/1/2025
ESTIMATE # 123
Expiry Date: 12/31/2025
Unit price Amount
$ 2.00 $ -
$ 2.00 $ -
$ 2.00 $ -
$ 4.00 $ -
$ - $ -
$ - $ -
$ - $ -
Subtotal $ 10.00
Credit $ 1.00
Tax 8.20%
Balance Due $ 9.74

Kickbacks & Bid-Rigging: The Collusive Scheme

- Kickbacks and bid-rigging involve illegal payments and manipulating competitive bidding processes.
- **Bid-Rigging:** Collusion among bidders (or between bidder and buyer) to manipulate the outcome of a competitive bidding process.
- **Types of Bid-Rigging:**
  - **Complementary Bidding:** Some bidders submit intentionally high bids to lose.
  - **Bid Suppression:** Some bidders agree not to bid.
  - **Bid Rotation:** Bidders take turns winning.
- **Impact:** Higher costs for grant projects, reduced quality, unfair competition, violation of procurement rules.

Misrepresentation of Costs: Hiding the Truth

- Misrepresenting costs involves falsifying or inflating expenses to make them appear allowable or eligible.
- **Common Tactics:**
  - Charging personal expenses as program costs.
  - Shifting costs between grants to hide overruns or unspent funds.
  - Inflating the value of in-kind contributions.
  - Categorizing administrative costs as direct program costs.
  - Charging expenses to a grant that occurred outside the grant period.
- **Impact:** Noncompliance, disallowance of costs, loss of funds.



Diversion of Funds: The Unauthorized Path

- This occurs when grant funds are used for purposes other than those specified and approved in the grant agreement.
- **Examples:**
  - Using funds intended for a specific program to cover general operating expenses.
  - Transferring grant money to unrelated projects or entities.
  - Investing grant funds in speculative ventures.
  - Using program funds for personal luxuries (e.g., luxury vehicles, lavish events).
- **Often a Result Of:** Weak financial controls, lack of oversight, or direct fraudulent intent.
- **Impact:** Failure to achieve grant objectives, loss of funding, legal repercussions.



Identity Theft (Grants Context): Stolen Trust

- Using stolen personal or organizational identities to apply for, receive, or misuse grant funds is a growing risk.
- **How It Happens:**
  - Using stolen Social Security numbers or EINs to create fake organizations.
  - Submitting grant applications under the name of a legitimate, but unsuspecting, individual or non-profit.
  - Impersonating a legitimate grantee to submit false invoices or reports.
- **Increasing Risk:** With more online applications and digital processes.
- **Impact:** Financial loss, reputational damage to the real entity, legal complications.



Fabricated Supporting Documentation: The Paper Trail of Lies

- Creating fake documents or altering genuine ones is a common way to support fraudulent claims.
- **Examples:**
  - Forging signatures on approvals or timesheets.
  - Creating fake invoices from nonexistent companies.
  - Altering dates, amounts, or descriptions on real receipts/invoices.
  - Producing false attendance records for program participants.
  - Manufacturing fake permits or licenses.
- **Often Used To:** Support false billing, ghost employee schemes, or misrepresentation of costs.
- **Impact:** Hinders legitimate oversight, provides false audit trails.

Grant Diversion for Personal Gain: The Ultimate Betrayal

- This is the direct and intentional redirection of grant funds by an individual for their personal benefit.
- **Differs from Misappropriation:** Often involves direct cash-outs or purchases for luxury items, distinct from subtle misuse of assets.
- **Examples:**
  - Purchasing personal vehicles, homes, or vacations with grant money.
  - Transferring large sums of grant funds directly to personal bank accounts.
  - Using grant credit cards for personal shopping sprees.
  - Paying off personal debts with grant funds.
- **Impact:** Complete loss of funds for the intended beneficiaries, severe legal consequences.



Conflict of Interest Abuses: Exploiting Influence

- Situations where personal interests conflict with professional duties can lead to unfair advantages and inflated costs.
- **Abuses in Grants:**
  - Awarding contracts to a company owned by a family member without competitive bidding or disclosure.
  - Hiring unqualified relatives or friends for grant-funded positions.
  - Purchasing goods/services from a company in which an approving official has a financial stake.
  - Grant review panel members giving preferential treatment to organizations with which they have personal ties.
- **Impact:** Unfair advantage, inflated costs, poor quality work, erosion of public trust.



Subrecipient Fraud: The Ripple Effect

- Fraudulent activities by an organization or individual receiving a subaward can have significant consequences for the prime grantee.

- **How It Happens:**
  - Subrecipient misrepresenting their capabilities in a proposal.
  - Subrecipient misusing funds or submitting false reports to the prime grantee.
  - Subrecipient colluding with vendors to inflate costs.
  - Subrecipient failing to deliver promised services while claiming reimbursement.

- **Challenge for Prime Grantees:** Monitoring and oversight are crucial.

- **Impact:** Prime grantee is ultimately responsible to the main grantor, leading to potential claw backs and reputational damage.

Data Manipulation/Reporting Fraud: Falsifying Performance

- Intentionally altering or fabricating data to misrepresent performance or justify continued funding is a serious scheme.

- **Examples:**
  - Inflating the number of people served by a program.
  - Falsifying outcomes data (e.g., success rates, impact metrics).
  - Modifying financial records to hide deficits or unallowable expenses.
  - Creating fictitious participant surveys or testimonials.

- **Impact:** Misleading reporting, wasted resources on ineffective programs, failure to achieve real impact.

Unallowable Costs: The Forbidden Expenses

- Charging expenses to a grant that are explicitly prohibited, or do not meet the criteria for allowability set forth by the grant agreement, regulations (e.g., Uniform Guidance), or generally accepted accounting principles, is a form of fraud if done deliberately.
- **Examples (Common Unallowable Costs):**
  - Alcoholic beverages.
  - Entertainment expenses.
  - Fines and penalties.
  - Lobbying costs.
  - Certain types of advertising or public relations costs.
  - Personal use of organization assets.
- **Fraud Connection:** Becomes fraud when *deliberately* disguised or misrepresented as allowable.
- **Impact:** Disallowance of costs, requirement to repay funds.



Travel Fraud: The Phantom Journey

- Misrepresenting travel expenses or claiming reimbursement for non-existent or non-grant-related travel is a common scheme.
- **Examples:**
  - Submitting inflated mileage claims.
  - Charging personal travel as grant-related travel.
  - Submitting fake receipts for accommodation, meals, or transportation.
  - Claiming per diems for days not actually spent on travel.
  - Traveling first-class when grant rules specify economy.
- **Red Flags:** Inconsistent travel patterns, lack of clear business purpose, missing documentation.
- **Impact:** Waste of grant funds, violation of travel policies.



Why Case Studies? Learning from Real Situations

- We'll use real-world examples to illustrate how these fraud schemes manifest in practice.
- **Purpose:**
  - Bring abstract concepts to life.
  - Show how different fraud schemes manifest in reality.
  - Highlight the red flags that were present.
  - Demonstrate the consequences of fraud.
  - Encourage critical thinking and discussion.
- **Note:** These are simplified for training; real cases are often more complex.

Case Study 1: The "Ghost Employee" Nonprofit - Scenario

- **Scenario:** "Harmony Haven," a small non-profit, received a grant for a youth mentorship program. The Finance Manager, Sarah, was responsible for payroll. Over two years, payroll expenses on the grant budget seemed slightly high, but no red flags were overtly noticed. Eventually, an anonymous tip to the board's newly established hotline alleged that 'John Doe,' a program coordinator listed on the payroll, had never actually worked for Harmony Haven.“

Case Study 1: The "Ghost Employee" Nonprofit - Fraud Scheme Unveiled

- **What Happened:** Sarah, the Finance Manager, had secretly added "John Doe" to the payroll system. She directed "his" direct deposits to a bank account she controlled. She also created fake timesheets and performance reviews for "John Doe" to support the payments. This scheme went undetected for nearly two years.

- **Scheme Type:** Ghost Employee (Asset Misappropriation).

Case Study 1: The "Ghost Employee" Nonprofit - Red Flags Present

- **Red Flags:**
  - **Behavioral:** Sarah's reluctance to take vacation, her insistence on handling all payroll tasks herself.
  - **Systemic:** Lack of segregation of duties (Sarah could add employees AND process payroll). Inadequate supervisor review of payroll reports.
  - **Financial:** Slightly high payroll costs for the number of reported staff; no physical presence of "John Doe."
  - **Response:** Anonymous tip (crucial for detection).

Case Study 1: The "Ghost Employee" Nonprofit - Lessons Learned

- **Lessons:**
  - **Segregation of Duties:** Critical for payroll and financial processes.
  - **Supervisor Review:** Managers must verify their team's payroll.
  - **Background Checks:** Verify all new hires thoroughly.
  - **Hotlines:** Provide a safe channel for reporting suspicions.
  - **Regular Audits:** Payroll reconciliation and review of active employees.

Case Study 2: The "Overbilling Contractor" University - Scenario

- **Scenario:** "Global Research University" received a substantial grant for a multi-year environmental study. They contracted with "EcoSolutions Inc." for specialized field equipment and support services. Mid-way through the project, the grant administrator noted that EcoSolutions' invoices seemed consistently higher than initial estimates for similar items from other vendors. The invoices often contained broad descriptions like "consulting services" without specific details.

Case Study 2: The "Overbilling Contractor" University - Fraud Scheme Unveiled

- **What Happened:** EcoSolutions Inc. was colluding with a university project coordinator. The coordinator would approve inflated invoices from EcoSolutions for services not rendered or at significantly higher prices than market rate. In return, the coordinator received a portion of the overbilled amount as a kickback.

- **Scheme Type:** False Billing/Invoicing, Kickbacks, Conspiracy to Defraud.

Case Study 3: The "Kickback King" Research Project - Red Flags Present

- **Red Flags:**
  - **Financial:** Consistently higher prices from one vendor; invoices with vague descriptions.
  - **Vendor:** New vendor with potentially limited history (if applicable in original scenario).
  - **Behavioral:** Project coordinator pushing for quick approvals, reluctance to share vendor details.
  - **Systemic:** Potential lack of competitive bidding or independent review of invoices.

Case Study 2: The "Overbilling Contractor" University - Lessons Learned

- **Lessons:**
  - **Vendor Due Diligence:** Thoroughly vet new vendors.
  - **Detailed Invoices:** Demand specific descriptions for all services/goods.
  - **Competitive Bidding:** Ensure a robust, fair procurement process.
  - **Price Comparisons:** Regularly compare vendor prices against market rates.
  - **Segregation of Duties:** Separate requisition, approval, and payment roles.

Case Study 3: The "Kickback King" Research Project - Scenario

- **Scenario:** "Innovate Labs" secured a large grant for a medical research project. Dr. Chen, the lead researcher, was responsible for procuring specialized lab equipment and supplies. He consistently favored a single supplier, "MedEquip Solutions," even when other suppliers offered more competitive pricing or faster delivery. Junior staff members occasionally noted that Dr. Chen seemed to have an unusually close relationship with MedEquip's sales representative.

Case Study 3: The "Kickback King" Research Project - Fraud Scheme Unveiled

- **What Happened:** Dr. Chen was receiving regular "kickbacks" from MedEquip Solutions in exchange for directing all of Innovate Labs' grant-funded purchases to them. These kickbacks were disguised as "consulting fees" or "referral bonuses" paid to a shell company controlled by Dr. Chen.

- **Scheme Type:** Kickbacks, Conflict of Interest Abuses.

Case Study 3: The "Kickback King" Research Project - Red Flags Present

- **Red Flags:**
  - **Vendor:** Consistent favoritism towards one vendor despite better alternatives.
  - **Financial:** Higher prices than market rate.
  - **Behavioral:** Unusually close relationship with a vendor, reluctance to consider other suppliers.
  - **Systemic:** Lack of competitive bidding or independent review of procurement decisions by Dr. Chen.

Case Study 3: The "Kickback King" Research Project - Lessons Learned

- **Lessons:**
  - **Strong Procurement Policies:** Enforce competitive bidding and vendor rotation.
  - **Conflict of Interest Disclosure:** Require regular, mandatory disclosure from all key personnel.
  - **Independent Review:** All significant procurement decisions should have independent oversight.
  - **Ethics Training:** Reinforce ethical purchasing practices.
  - **Vendor Due Diligence:** Periodically review vendor performance and pricing.

Case Study 4: The "Diverted Funds" Community Organization - Scenario

- **Scenario:** "Safe Neighborhoods Now," a small community non-profit, received a grant to implement a violence prevention program. The Executive Director, Ms. Davis, had sole control over the organization's bank accounts and approved all expenditures. Over several months, the program seemed to struggle, but Ms. Davis consistently reported significant progress and high expenditures. Bank statements later revealed large, frequent withdrawals from the grant account labeled "misc. expenses.“

Case Study 4: The "Diverted Funds" Community Organization - Fraud Scheme Unveiled

- **What Happened:** Ms. Davis systematically diverted large portions of the grant funds for her personal use, including lavish travel, personal shopping, and paying off her credit card debts. She concealed this by submitting falsified financial reports to the grantor, overstating program expenditures and fabricating participant numbers to suggest the program was thriving.

- **Scheme Type:** Diversion of Funds, Financial Reporting Fraud, Fabricated Supporting Documentation.

Case Study 4: The "Diverted Funds" Community Organization - Red Flags Present

- **Red Flags:**
  - **Systemic:** Lack of segregation of duties (sole control over finances), lack of oversight from the board.
  - **Financial:** Large, vague "misc. expenses," significant cash withdrawals.
  - **Behavioral:** Ms. Davis's complete control, potentially resisting scrutiny.
  - **Performance:** Program struggling despite high reported expenses.

Case Study 4: The "Diverted Funds" Community Organization - Lessons Learned

- **Lessons:**
  - **Strong Board Oversight:** Active and engaged board with financial literacy.
  - **Segregation of Duties:** Never allow one person sole control over finances.
  - **Detailed Expense Documentation:** Require receipts and clear justifications for all expenditures.
  - **Independent Financial Reviews:** Regular, external audits are crucial.
  - **Robust Performance Monitoring:** Verify reported progress with actual activities.

Case Study 5: The "Falsified Research Data" Scientist - Scenario

- **Scenario:** Dr. Anya Sharma, a respected research scientist, received a significant grant to develop a new diagnostic tool. Under pressure to publish groundbreaking results and secure follow-on funding, her lab's reported data consistently showed highly positive outcomes, often exceeding expectations. A junior researcher, reviewing raw data files, noticed some inconsistencies that didn't align with the published results.

Case Study 5: The "Falsified Research Data" Scientist - Fraud Scheme Unveiled

- **What Happened:** Dr. Sharma, or someone under her direct instruction, had deliberately altered raw data files and statistical analyses to create a more favorable outcome for the diagnostic tool. This allowed her to publish seemingly successful results, impress the grantor, and position herself for additional funding, despite the tool not performing as claimed.

- **Scheme Type:** Data Manipulation/Reporting Fraud, False Statements/Representations.

Case Study 5: The "Falsified Research Data" Scientist - Red Flags Present

- **Red Flags:**
  - **Performance:** Consistently "too good to be true" results, always exceeding expectations.
  - **Behavioral:** Pressure to publish, potential defensiveness around raw data.
  - **Documentation:** Inconsistencies between raw data and reported data.
  - **Systemic:** Lack of independent data verification or peer review of raw data.

Case Study 5: The "Falsified Research Data" Scientist - Lessons Learned

- **Lessons:**
  - **Data Integrity Policies:** Strict protocols for data collection, storage, and analysis.
  - **Independent Verification:** Require independent review of raw data for high-stakes projects.
  - **Ethical Research Training:** Emphasize academic integrity and consequences of misconduct.
  - **Pressure Management:** Address unrealistic expectations for results.
  - **Whistleblower Protection:** Encourage ethical reporting from within the research team.

Interactive Exercise: "Which Scheme Is This?" - Instructions

- Now, let's test your ability to identify various fraud schemes in short scenarios.
- **Instructions:** We'll present several short scenarios. Your task is to identify the most likely fraud scheme(s) at play based on what you've learned. Be ready to explain your reasoning!

Scenario 1 (Exercise): The Unpaid Subcontractor

- **Scenario:** "A grant funds construction of a community center. The prime contractor submits invoices for a specific subcontractor, and payments are made. However, the subcontractor later complains they haven't been paid for months, despite invoices showing they were. Investigation reveals the funds were routed to a different, newly created company with a very similar name."

- **Question:** What scheme(s) do you suspect?

Answer 1 (Exercise): The Unpaid Subcontractor

- **Most Likely Scheme(s):**
  - **Diversion of Funds:** Funds intended for the subcontractor were sent elsewhere.
  - **False Billing/Invoicing:** Invoices might have been manipulated to direct payments to the fraudulent entity.
  - **Identity Theft (of the subcontractor's name/details):** If the new company truly mimicked the subcontractor's identity.

Scenario 2 (Exercise): The Inflated Consultant Hours

- **Scenario:** "A marketing consultant is hired for a grant-funded campaign. Their invoices consistently show 40 hours per week, even during periods when the project team observed minimal activity. The project manager, who approves the invoices, is frequently seen having expensive lunches with the consultant."

Answer 2 (Exercise): The Inflated Consultant Hours

- **Most Likely Scheme(s):**
  - **False Billing/Invoicing:** Charging for hours not worked.
  - **Kickbacks:** The expensive lunches could indicate a quid pro quo for approving inflated invoices.
  - **Conflict of Interest:** If there's an undisclosed personal or financial relationship between the consultant and project manager.

- **Discussion:** What red flags are present here?

Scenario 3 (Exercise): The Missing Equipment

- **Scenario:** "A grant provides funds for specialized equipment for a community technology center. Purchasing records show the equipment was bought and paid for. However, during a routine inventory check, several high-value items are missing, and there's no record of them being deployed, used, or discarded."
- **Question:** What scheme(s) do you suspect?

Answer 3 (Exercise): The Missing Equipment

- **Most Likely Scheme(s):**
  - **Theft / Misappropriation:** The equipment was likely stolen or used for unauthorized purposes.
  - **Ghost Vendor (possible):** If the equipment was never truly purchased, but records show it was, implying a fake vendor.
  - **False Billing/Invoicing (possible):** If the equipment was paid for but never delivered.

- **Discussion:** What internal controls could have prevented this?

Module Summary & Key Takeaways

- To summarize, understanding common fraud schemes is essential for anticipating and preventing deception.
- **Recap:**
  - Fraud schemes are the active methods used to commit fraud.
  - Common schemes include ghost employees/vendors, false billing, kickbacks, and fund diversion.
  - Real-world case studies illustrate how these schemes unfold and their consequences.
  - Recognizing these patterns is vital for both prevention and detection.
- **Action Item:** Be aware of the common tactics. Consider how these schemes might occur in your own grant-funded activities.