Anti-Money Laundering, Fraud, and Elder Abuse Presentation
Hello, I’m your presenter today, Caroline!

- I have over five years of experience in the Anti-Money Laundering (AML) and Fraud industry.
- I am a Certified Anti-Money Laundering Specialist (CAMS) and have a B.S. and M.A. in Criminal Justice.
- Prior to my employment with Western Alliance Bank, I was employed with:
  - MUFG Union Bank and American Express as an AML/Fraud Investigator
  - The Better Business Bureau as an Investigator
  - An Intern with the State Senate in Arizona.
Disclaimer

The views expressed herein are those of the presenter and do not necessarily reflect the views of Western Alliance Bancorporation or its subsidiaries.
Agenda

• Purpose
• About Western Alliance Bank
• Money Laundering
• Fraud
• Elder Abuse
• Resources
• Q & A
Purpose

- To define and explain money laundering and money laundering schemes;
- To define and explain fraud and various types of fraudulent activity/schemes;
- To define and explain elder abuse;
- How to identify “Red Flag” indicators regarding money laundering, fraud, and elder abuse;
- What to do when you see these indicators;
- How to report unusual activity and resources available.
About Western Alliance Bank

With more than $25 billion in assets, Western Alliance Bancorporation (NYSE: WAL) is one of the country’s top-performing bank holding companies. Its primary banking subsidiary, Western Alliance Bank, Member FDIC, helps business clients realize their growth ambitions with local teams of experienced bankers who deliver superior service and a full spectrum of customized loan, deposit and treasury management capabilities.

Business clients also benefit from a powerful array of specialized financial services that provide strong expertise and tailored solutions for a wide variety of industries and sectors. A national presence with a regional footprint, Western Alliance Bank operates individually branded, full-service banking divisions and has offices in key markets nationwide. For more information, visit westernalliancebank.com.
PART I: Money Laundering
What Is Money-Laundering?

To put it simply, money laundering is taking “dirty money” obtained from illegal activities and via a process of financial transactions, “cleaning” the money, so it appears legitimate.

The three stages of money laundering are placement, layering, and integration and they work like this:
Embezzlement

There are many types of money laundering that may impact the public and private sector, including embezzlement. Embezzlement is “the theft or the misappropriation of funds placed in one’s trust or belonging to one’s employer.”

Anything can be subjected to embezzlement, including cash, checks, and even office supplies!
Embezzlement Red Flags

To prevent embezzlement and to spot red flags, Quickbooks suggests you:

• Monitor cash via RFID’s, barcodes, and/or by itemizing as to compare leftover funds to sales receipts to spot shortages easily.
• Make receipts mandatory for reconciliation purposes.
• Review bank accounts monthly; ensure that checks and deposits are signed or conducted by at least two people.
• Verify dates of payments against corresponding deposit dates.
• Tag equipment with a unique code, have a master list of assigned equipment, and verify periodically that equipment is with the assigned employee.
• Limit access to office supplies; have a log of when items are requested, by whom, and why in order to see if patterns emerge.
• Double check receipts against any petty cash amounts, confirm that petty cash amounts are reasonable, and have a banking alert set up for anything over the “reasonable” amount.
Embezzlement Resources

Report *embezzlement* to:

- The City Manager/Board of Directors;
- Your financial institution;
- Your insurance company, as some insurance policies cover loss due to employee theft;
- The IRS;
- Local Police;
- Your FBI field office
  - use this to locate field offices: https://www.fbi.gov/contact-us/field-offices.
Investment Schemes

Other types of money laundering include investment schemes.

Examples of common investment schemes, per the FBI, include:

**Ponzi schemes** which work by utilizing new investors’ money to pay out older investors.

In **pyramid schemes** victims are tasked to recruit more victims via the payment of recruitment commissions; these schemes earn their profits not by the sale of goods, products, or services, but instead by the sale of new distributorships.
Investment Schemes Red Flags

If you make decisions regarding investments, 401k, and pension plans, be sure to conduct an audit of earnings statements, and if you are considering looking in to a new investment firm that is not well known, the FBI suggests you:

✓ Ask about the terms and conditions.
✓ Check the broker/financial advisor’s license through FINRA and the SEC.
✓ Be cautious when responding to offers received through unsolicited E-mail or from a foreign entity.

If you feel you have been a victim of an Investment Scheme, USA.gov suggests the following:

✓ File a complaint with the Securities and Exchange Commission (SEC).
✓ Report pyramid or Ponzi schemes to the Federal Trade Commission (FTC).
✓ Report AZ companies to the Corporation Commission Securities Division, (602) 542-4242.
PART II: Fraud
What is Fraud?

Fraud is defined by the FBI as intentionally lying for the purpose of convincing another person or entity to surrender something of value or give up a legal right.
E-mail Compromise and Phishing

An **E-mail Compromise** occurs when an attacker gains access to an e-mail account and spoofs the owner of the account’s identity to defraud a company, employee, customer, or other individual of money.

**Phishing** is similar to an E-mail Compromise. In phishing attacks, an e-mail or text message is received, appears to be from a known vendor, well-known entity, or appears to be sent from within the company/city. It is not a real e-mail and usually contains a malicious link which will then infect your computer with a virus or lead you to unintentionally provide confidential information such as a password or PIN.
E-mail Compromise/Phishing Red Flags

Look Out For:

- Broken sentence structure, improper punctuation, and spelling errors.
- Use of the word “kindly”.
- If an e-mail address looks off, look for details first: bobbysueconstruction@gmail.com VS bolbysueconstruction@gamail.com.
- Statement that they cannot be contacted on the phone without you stating you will call.
E-mail Compromise/Phishing Resources
If you believe you, your company, or city has been subjected to an E-mail Compromise or Phishing Attack, you should:
• Consult with your IT department to determine the extent of the damage and bring in cybersecurity experts who can test not only e-mails but the rest of your network.
• Report it to your insurance company as some offer cyber insurance. If you don’t have this type of policy, you may want to consider purchasing it.
• Notify local and federal police.
• Inform and notify customers in writing if their information was compromised as this is required by law.
• Comply with your regulating bodies.
• Have a contingency plan for how to operate, such as having a backup network and two-factor authentication.
Check Fraud

Check fraud is the “...unlawful use of checks to illegally acquire or borrow funds that do not exist within the account balance of account-holder’s legal ownership.”

To prevent check fraud... employees should “check” the details prior to depositing/accepting...
Computer Virus Scams

Computer virus scams are also known as a tech support scam. According to the Federal Trade Commission, scammers will use pop-up messages on your computer, claim to be techs from Microsoft/Apple, ask you to give them remote access to your computer, and then ask you to pay for unnecessary services.

If you get an unexpected message, STOP! Do not click on any links, don’t give control of your computer, and don’t send money. If you suspect you were scammed:

- Get rid of malware via a legitimate security software and contact your IT department;
- Immediately change your passwords;
- Consider reporting the scam to ftc.gov/complaint.
PART III: Elder Abuse
Types of Elder Abuse

In Arizona, per the Arizona Attorney General’s website there are the following types of elder abuse: Physical, Emotional, Sexual, Financial, and Neglect.

Financial Elder Abuse is the most common; it is the illegal or improper use of a vulnerable adult or his/her financial resources for another's profit or advantage.
How To Prevent Elder Abuse-Communities

According to HealthinAging, communities should:

• Create community supports and services for caregivers and older people that reduces the risk factors tied to elder abuse, such as isolation.
• This may include services such as meals on wheels or social groups, like book clubs for seniors.
• Identify ways to empower the elderly through senior centers and programs that will reduce ageism.
• Examples include offering age appropriate courses at the library, community colleges, and recreation centers for seniors.
Elder Abuse Resources

Though cities in AZ are not mandatory Elder Abuse reporters, if you see something, it is always a good idea to say something. If you suspect someone else is a victim of elder abuse, contact: in an emergency- 9-1-1 or the police; for non-emergency physical abuse- (877) SOS-ADULT or (877) 767-2385 - Adult Protective Services (APS); (602) 264-HELP or (602) 264-4357 - Area Agency on Aging 24hr Helpline; (844) 894-4735 or (602) 542-2124 - Attorney General's TASA Helpline; and for financial exploitation-(844) 894-4735 or (602) 542-2124 Attorney General's TASA Helpline.

These numbers and additional resources can be found on the handout.
Sources

Bing Dictionary

https://quickbooks.intuit.com/r/money/stop-embezzlement-before-it-drains-your-small-business/

https://www.wikihow.com/Report-Embezzlement


