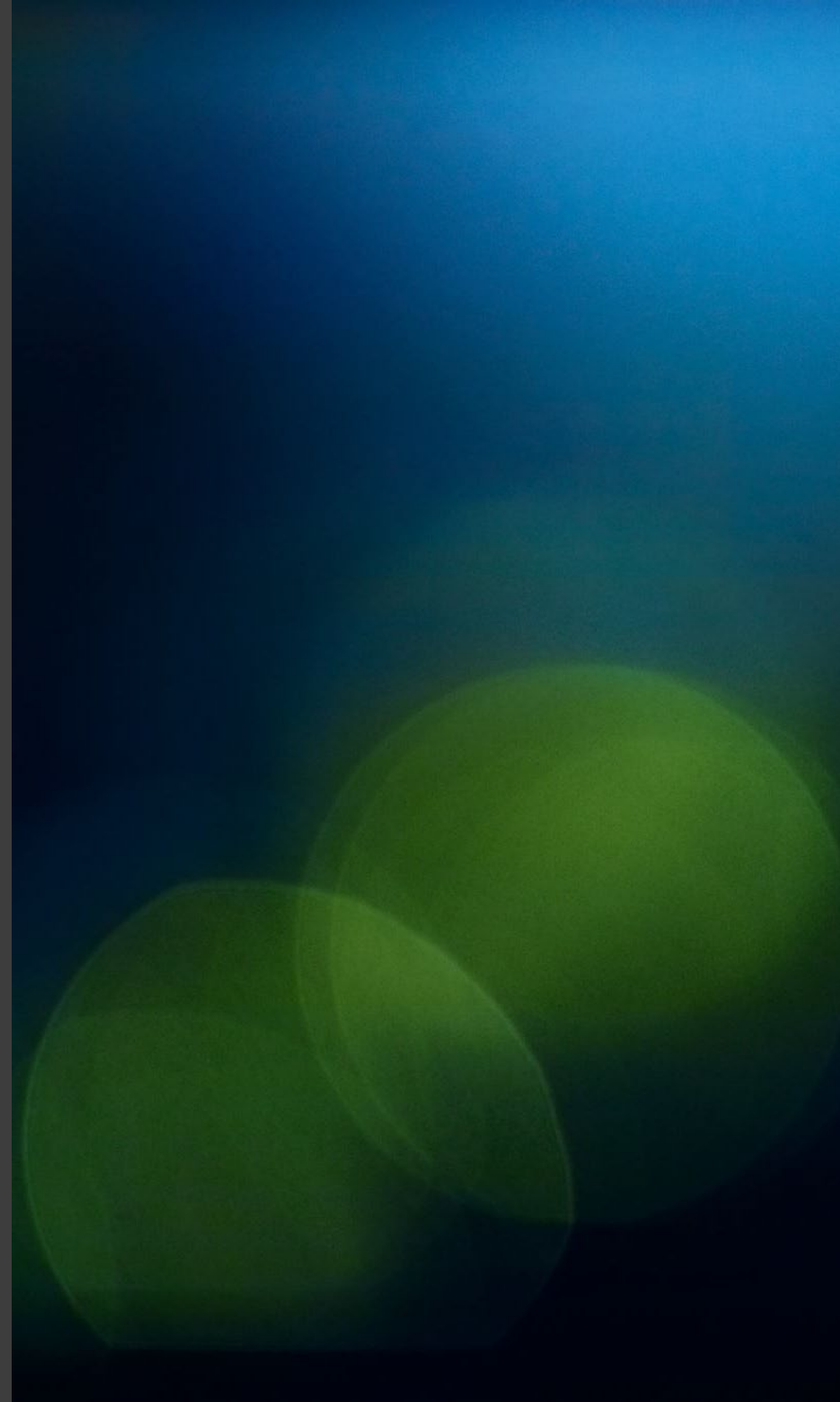
HAS COVID-19 INFECTED YOUR BSA PROGRAM?

WESTERN BANKERS ASSOCIATION

2020 REGULATORY COMPLIANCE, VIRTUAL CONFERENCE

OCTOBER 6, 2020



PRESENTERS

RADHIKA DHOLAKIA-LIPTON,

CEO/PRESIDENT

RADD LLC. RISK ADVISORY, CONSULTING AND INTERNAL AUDIT FIRM

ELIZABETH ("LIZ") SLIM, CAMS AND

SENIOR CONSULTANT

THE VOLKOV LAW GROUP, LLC

AGENDA

- Frauds and Scams
- How has your BSA program changed due to COVID-19
- Training during the pandemic
- BSA/AML Program guidance issued by government agencies

New and familiar areas of risk:

- PPP Loan Fraud
- Cyberattacks
- Unemployment Scams
- Other Scams & Schemes

COVID-19 FRAUD

PPP LOAN FRAUD

- The DOJ has actively charged people they suspect to have fraudulently obtained Paycheck Protection Program and Economic Injury Disaster loans from the SBA.
- Over $1 billion has gone to companies that "double dipped" and received multiple PPP loans in violation of rules, according to congressional report. The subcommittee found over 10,000 loans in which the borrowers obtained more than one loan.
- Over 600 loans, for nearly $100 million, went to companies that had been barred from doing business with the government.

PPP LOAN FRAUD (CONTINUED)

- Suspects have used loan proceeds to enrich themselves. To execute their schemes, suspects have presented fake tax returns, bank statements, payroll numbers, and fake or synthetic identities. They have also used shell companies.
- According to a July report from the SBA's Office of Inspector General, the agency's investigative division has received reports from nearly "440 financial institutions ranging from small, local credit unions to major national institutions."

PPP LOAN FRAUD RED FLAGS

- PPP applications with manipulated or fraudulent supporting documentation.
- PPP applications in different names that contain nearly identical application information and supporting documents. and originate from the same Internet Protocol (IP) address.
- Fake businesses established during the pandemic that do not have an internet presence, with minor differences. between names on the application documents and public business registration documents.

PPP LOAN FRAUD RED FLAGS (CONTINUED)

- Existing accounts may have a consistently low balance with no history of payroll expenses.
- New accounts applying for SBA funds. These accounts do not reflect any previous business-related transaction activity, and funds are quickly transferred after receiving loan advances or proceeds.
- After loan advances or proceeds are deposited into an account, funds are immediately withdrawn in cash, wired out, transferred to an investment account, used to purchase luxury assets not associated with typical business-related expenses, or used to start an entirely new business.

CYBER FRAUD AND ATTACKS

- Based on FinCEN's July 30 advisory on cybercrime and cyber-enabled crime, community financial institutions need to retune their transaction monitoring rules and thresholds to capture new illicit financial patterns.
- The key theme during the COVID-19 pandemic is the enterprises' mass-migration towards remote access for employees. This shift has given cybercriminals ample opportunity "to exploit financial institutions' remote systems and customer-facing processes."
- Cybercriminals and malicious state actors are targeting vulnerabilities in remote applications and virtual environments to steal sensitive information, compromise financial activity, and disrupt business operations, says FinCEN.

CYBER FRAUD AND ATTACKS (CONTINUED)

The key issue that emerges here is the resilience of Know Your Customer and transaction:

- Digital manipulation of Identity documentation
- Leveraging compromised credential across accounts
- Use of anti-detect browsers that mimic user's digital footprint

CYBER RED FLAGS – INCLUDE IN YOUR REVIEW PROCESS

- Name spelling in account information does not match the government-issued identity documentation provided for online onboarding.
- Pictures in identity documentation, especially areas around faces:
  - are blurry, low resolution, or have aberrations.
  - Pictures or other images of persons show visual signs indicating possible image manipulation
  - Images visual irregularities that indicate digital manipulation of the images, especially around information fields likely to have been changed to conduct synthetic identity fraud (e.g., name, address, and other identifiers

CYBER RED FLAGS – INCLUDE IN YOUR REVIEW PROCESS (CONTINUED)

- A customer's physical description does not match ID or other images of the customer.
- Customer logins occur from a single device or Internet Protocol (IP) address across multiple seemingly unrelated accounts, often within a short period of time.
- Customer logins occur within a pattern of high network traffic, decreased login success rates and increased password reset rates.
- Customer contacts financial institution to change account communication methods and authentication information, and quickly attempts to conduct transactions to an account that never previously received payments from the customer.

UNEMPLOYMENT INSURANCE FRAUD

- The CARES Act provides additional unemployment insurance funding for eligible individuals through the Pandemic Unemployment Assistance (PUA) program, the Federal Pandemic Unemployment Compensation program (FPUC), and the Pandemic Emergency Unemployment Compensation (PEUC) program.
- UIBs can be disbursed using different mechanisms, such as debit cards or direct deposits. Risks and fraud schemes can vary significantly based on inherent risks posed by the particular mechanism used to receive the funds.

UNEMPLOYMENT INSURANCE FRAUD (CONTINUED)

- Fraudsters could pocket $26 billion in unemployment insurance benefit (UIB) scams, according to the Department of Labor's OIG.
- Scammers are stealing people's identities to file for unemployment insurance under their name.
- States' reliance on "self-certification alone to ensure eligibility for PUA will lead to increased improper payments and fraud," according to the DOL OIG report.

UNEMPLOYMENT INSURANCE FRAUD RED FLAGS

- An account receiving unemployment insurance benefits from another state without a reasonable explanation, or from multiple other states other than where the individual resides.
- An account receiving unemployment insurance benefits on behalf of multiple individuals.
- New or established accounts are opened, but they lack transactional activity. Then they are suddenly used to collect unemployment insurance benefits

UNEMPLOYMENT INSURANCE FRAUD RED FLAGS (CONTINUED)

- Imposter schemes, where a fraudster poses as an official entity to defraud victims, such as obtaining personally identifiable information to fraudulently file for unemployment insurance benefits.
- Money mules, where an individual knowingly or unknowingly obtains money on behalf of, or at the direction of, someone else to improperly obtain unemployment insurance benefits

Community FI's need to take a risk-based approach, verifying identity is everything!

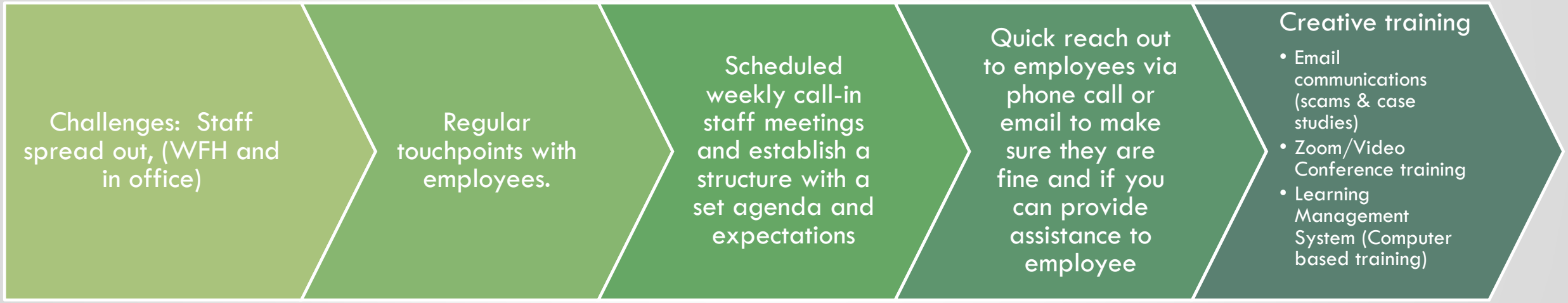
NEW ADAPTIONS TO BSA/AML PROGRAM DUE TO PANDEMIC

- CTR filings decline
- PPP loan frauds increase
- Unemployment benefits paid
- Cash withdrawals by customers (panic driven)
- Mobile Banking transactions increased
- Financial fraud on the rise
- Sanctions program must be maintained

NEW ADAPTIONS TO BSA/AML PROGRAM DUE TO PANDEMIC, CONTINUED

- How does this affect your staffing model?
- How does this affect your Transaction Monitoring System?
- If new alerts produced large amount of results, consider conducting a lookback review.
- How "Effective" is your program?

TRAINING AND COMMUNICATIONS DURING PANDEMIC



GOVERNMENT GUIDANCE ISSUED

Do not ignore guidance issued by regulatory agencies during the pandemic.

- ***Review*** the publications to determine if you need to make adjustments to your BSA/AML program and risk assessment.
- ***Communicate*** the published guidance to the Board of Directors and Management how this affects your BSA/AML program and what you have done to ensure the compliance program meets the new guidance, if it applies.

LIST OF GOVERNMENT GUIDANCE ISSUED

- 04/15/2020: FFIEC revised BSA/AML Examination Manual and Procedures
- 08/03/2020: FinCEN issued CDD FAQs
- 08/18/2020: FinCEN and Interagencies issued a statement on BSA Enforcement Actions
- 08/21/2020: FinCEN and Interagencies issued a statement on CDD requirements for Political Exposed Persons (PEPs)
- 09/14/2020: FinCEN issues Final Rule to Require CIP, AML and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator

1. Train and communicate staff on cyberattacks, fraud and scams that are on the rise during the pandemic.
2. Maintain reach-outs to employees working from home or the office to provide assistance and ensure they are doing well.
3. Review your BSA/AML program to determine if any adjustments should be made to your program, risk assessment and Transaction Monitoring System due to an increase or decrease of transactions in cash, money remittance and delivery channel (mobile banking, Debit/Credit card, Person-2-Person transactions, etc.). Restructure your AML teams to cross-train and provide coverage.
4. Don't forget to review publications/guidance/advisory issued by regulatory agencies that apply to OFAC Sanctions and BSA/AML regulations that may affect your compliance program.
5. Communicate issues to Board and Management

RESOURCES

- FinCEN Coronavirus Updates: https://www.fincen.gov/coronavirus
- FBI COVID-19 Updates: https://www.fbi.gov/coronavirus
- Department of Justice (DOJ) COVID-19 Fraud Updates: https://www.justice.gov/coronavirus/combattingfraud
- FTC COVID-19 Updates: https://www.ftc.gov/coronavirus/scams-consumer-advice
- FFIEC Info base: BSA/AML Examination Manual revised 04/15/20: https://bsaaml.ffiec.gov/
- FinCEN FAQs Regarding CDD Requirements for Covered Financial Institutions: https://www.fincen.gov/sites/default/files/2020-08/FinCEN%20Guidance%20CDD%20508%20FINAL_2.pdf
- FinCEN Statement on Enforcement of the Bank Secrecy Act: https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf
- FinCEN and Agencies Issue Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons: https://www.fincen.gov/sites/default/files/shared/PEP%20Interagency%20Statement_FINAL%20508.pdf
- FinCEN Issues Final Rue to Require Customer Identification Program, Anti-Money Laundering Program, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator: https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-require-customer-identification-program-anti-money

CONTACT INFORMATION

RADHIKA LIPTON,
CEO/PRESIDENT

RADD LLC. RISK ADVISORY, CONSULTING AND INTERNAL AUDIT FIRM

EMAIL: radhika@raddllc.com

PHONE: (714) 624-8222

ELIZABETH SLIM, CAMS AND SENIOR CONSULTANT

THE VOLKOV LAW GROUP, LLC

EMAIL:
eslim@volkovlaw.com

PHONE: (626) 318-71553

QUESTIONS