2019 EDUCATION SCHEDULE

A Secura Member Benefit

Serving Financial Institutions and FinTech Companies

Through Risk Management and Strategy

Stay Compliant, Focused and Competitive.

- FINANCIAL INSTITUTION RISK MANAGEMENT
- FINTECH RISK MANAGEMENT
- FRAUD IDENTIFICIATION & PREVENTION
- REGULATORY & COMPLIANCE SERVICES
- RISK MANAGEMENT EDUCATION

Secura Risk Management, LLC.
800.515.8617
support@securariskmanagement.com

Not a Member? Check out all the benefits!

www.SecuraRiskManagement.com

2019 Secura Risk Management Webinars

The 2019 Webinars offered through Secura Risk Management provide members the ability to learn the most pressing risk management issues associated with payments, fraud, BSA/AML, cybersecurity, insurance considerations and regulatory requirements and expectations.

ACH Originator and Third-Party Sender Training on the 2019 *NACHA Operating Rules* Changes and Fraud Trends: Each year, the National Automated Clearing House Association (NACHA) publishes its Rules that outline the requirements for all participating depository financial institutions participating in the ACH network. A requirement in accordance with the *NACHA Operating Rules* is to educate ACH Originators and Third-Party Senders on their obligations under the Rules. This webinar will focus on the 2019 Rules changes that mostly impact ACH Originators and Third-Party Senders. There will also be a focus on fraud trends and targeted fraud on ACH Originators and Third-Party Senders including business account compromise, social engineering, phone forwarding, and other fraud trends that can have a negative impact on your ACH Originator and Third-Party Sender.

Topics covered:

- Expansion of Same Day Deadlines
- Dollar limit increase for Same Day ACH
- Other 2019 and 2020 NACHA Rules Changes and Initiatives
- Existing ACH Originator and Third-Party Sender top obligations for complying with the *NACHA Operating Rules*
- Top fraud trends in ACH that have significantly increased reputational and financial risk for ACH Originator and Third-Party Senders

Best Business Practice Document Included:

✓ This webinar will include a best business practice document for ACH Originators and Third-Party Senders to add to their daily operational procedures as reminders for compliance with existing and 2019 *NACHA Operating Rules Changes.*

Who Should Attend?

- ACH Originators
- ACH Third Party Senders
- Account Officers
- Relationship Managers
- Treasury Managers
- Electronic Banking Management/Staff
- Deposit Operations Management/Staff
- Risk Management
- Internal Auditors
- Compliance Management/Staff
- Senior Management

Date: January 7, 2019
Time: 2:00 – 3:00 p.m. EST

Best Business Practices for Risk Rating Your Treasury Clients: Regulatory guidance and network rules require that financial institution perform appropriate due diligence prior to approval. Financial institutions struggle with understanding how to effectively risk rate their treasury clients based on products and services, financial status, bank statement history, transactional risk reviews, and the ability to meet BSA standards. This webinar will focus on how to risk rate the customers using a risk rating methodology that takes into considerations all types of risks and assists treasury officers and relationships managers on appropriately risk rating, setting exposure limits and pre-determining when the periodic review should be performed based on the risk rating of the customer at the beginning and throughout the duration of the relationship.

Topics covered:

- Regulatory and network requirements for ACH, RDC, Wires, Lockbox and other Treasury Services;
- Review of each recommended risk criteria;
- Best business practices for risk scoring;
- Using a risk methodology approach for performing periodic reviews;
- How to more practically assess treasury services risks.

Who Should Attend?

- Account Officers
- Treasury Officers
- Relationship Managers
- Electronic Banking Management
- Compliance
- Internal Audit
- Risk Management

Best Business Practice Document Included:

☑ Sample Treasury Services risk scoring matrix

Date: January 22, 2019
Time: 2:00 – 3:00 p.m. EST

The Top Corporate Customer Fraud Threats and Mitigation Tools: Don't Wait until It's Too Late!
Your corporate customers are being targeted by fraudsters every day. From social engineering attacks to malware attacks, corporate customers are surrendering their sensitive information more than ever and are feeling the monetary pain of such attacks. This webinar will focus on the top fraud threats that are targeting corporate corporates and how these clients can mitigate the risks associated with monetary loss and/or reputational risk. This is a great webinar to pass along to your corporate customers to prepare them for such attacks.

Topics include:

- Social Engineering

- Specific fraud attacks (Wires, ACH, Checks and cross channel payments attacks such as foreign collection checks and outgoing wire transfers)
- Account Takeover
- Identity Theft
- Synthetic Identity
- Insurance Coverage for Corporate Account Fraud
- This webinar will also focus on how your corporate customers can prepare in terms of business continuity, incident response, and ensuring they have the right insurance coverage based on these increased threats.

Best Business Practice Document Included:

☑ Best business practice document for Corporate Customers including tips to ensure insurance coverage is enough based on increased fraud threats.

Who Should Attend?

- Corporate Customers of Financial Institutions
- Fraud Managers
- Risk Managers
- Operations Managers
- Front-Line Staff
- Back-Office Staff
- Compliance/Risk Management
- Internal Auditors
- Senior Management
- Legal Staff

Date: February 6, 2019
Time: 2:00 – 3:00 p.m. EST

Call Center/Client Facing Fraud Management: Important Red Flags for Identifying Fraud:

Call centers and departments responsible for receiving customer calls are feeling the increasing numbers of fraud attempts and have even been the victims of fraud through social engineering and other types of fraud threats. The goal of a financial institution is to ensure the customer has a positive experience; however, the fraudsters make it difficult by taking additional unnecessary time in attempting to overtake the call and socially engineer the customer service representative into breaking the rules, initiating an unauthorized transaction or surrendering sensitive information. This webinar will take attendees through leading business practices for identifying red flags for personnel taking calls to quickly identify a possible fraudster, how to handle fraud situations and how to map out your different call paths to ensure that the organizational structure is in place that also quickly identifies out of ordinary calls and/or requests. This webinar is a great session for training your front-line staff, customer call centers and/or any department that receives high volumes of customer inquiries.

Topics include:

- Fraud threats and trends in call centers such as spoof caller ID, Skype or Google Voice and other fraud attacks

- Best business practices for the Identification of a true customer vs. a fraudster
- How to handle fraudsters once identified
- Authentication practices for verifying the identity of the caller
- Organizational design of a call center to take into consideration significant increase in fraud threats
- Best business practices for training your client facing teams

Who Should Attend?

- Call Center Management
- Branch Management
- Information Security Officers
- Account Officers
- Treasury Officers
- Relationship Managers
- Compliance
- Internal Audit
- Risk Management

Best Business Practice Document Included:

☑ Sample Treasury Services risk scoring matrix

Date: February 7, 2019
Time: 2:00 – 3:00 p.m. EST

Improving your Internal Audits: Quality Assurance and Improvement for Smaller Financial Institutions: This session will walk through the results of a real-life external quality assessment and the follow up remediation to gain general conformance with the Auditing Standards. This session will also review the most common non-conformance issues with IIA Standards noted in external quality assessments and provide sample templates of the internal Quality Assurance and Improvement Program.

Topics Covered:

- Defining Quality Assurance and Improvement?
- Non-conforming issues?
- Quality Assessments

Who Should Attend?

- Internal Auditors
- Risk Managers
- Compliance Officers
- Senior Management
- Legal Staff

Date: February 8, 2018

Time: Noon – 1:00 p.m. EST

Co-Sourcing vs Outsourcing Internal Audit Arrangements: Even in larger financial institutions, there may be gaps in expertise and resource. This session will focus on the distinction between co-sourcing and outsourcing. Financial institutions embrace the concept of supplementing resources in different ways, including co-sourcing that serves as more of a partnership between internal audit staff and externally hired professionals to assist in the internal audit program.

Topics Covered:

- Difference between co-source and outsource and the benefits of both?
- Why do internal audit departments co-source or outsource?
- How does the program work?

Who Should Attend?

- Internal Auditors
- Risk Managers
- Compliance Officers
- Senior Management
- Legal Staff

Date: February 8, 2018
Time: 2:00 – 3:00 p.m.

How to Embrace Regulatory Technology (RegTech) for Improving your Risk Management Programs: This webinar will provide attendees an understanding of the importance of moving from a manual risk management environment to a more enhanced automated rules-based risk program. This webinar is perfect for financial institutions worried about how to keep up with compliance requirements while still working with excel spreadsheets, depending on one or a few individuals to get through audits and implement new regulations and having to go to different systems to obtain data for reporting purposes. This webinar will focus on the top compliance automation and how to effectively implement and significantly improve your efficiencies while strengthening risk management and internal controls.

Topics include:

- Vendor management technology
- Regulation E Error Resolution technology and workflows
- Customer Identification Program exception workflows
- Risk assessment technology and workflows
- Policy and procedure technology management
- Board reporting technology and management
- Internal audit technology and management

Who Should Attend?

- Compliance Officers
- Risk Managers
- Information Technology Officers
- Enterprise Risk Officers
- Internal Auditors
- CEOs/COOs
- Executive Management

Date: March 5, 2019
Time: 2:00 – 3:00 p.m. EST

Account Officer Training on ACH/RDC Credit and Transactional Underwriting, Setting Exposure Limits and Performing Periodic Reviews Efficiently and Effectively: Account officers/relationship officers may not understand the regulatory requirements for assessing the risks of ACH and RDC clients. What is the difference between credit underwriting and transactional risk underwriting? How do you set exposure limits while complying with regulatory requirements and ensuring that periodic reviews are performed in accordance with network rules and regulatory expectations? This webinar will take a deep dive from the time potential ACH and RDC customers are brought to the financial institution for review and approval through the duration of the relationship. Learn regulatory guidance, expectations and practical methods for complying while not forcing inefficient processes and inconveniences for the client.

Topics include:

- Best business practices for differentiating between credit underwriting and transactional underwriting
- Providing a practical business practice for setting effective exposure limits
- Providing an understanding of how to effectively monitor and perform your periodic risk reviews
- Following effective and efficient methods for handling over-limit activity
- Understanding Red flags to help you identify that an account or accounts may have increased risk and when to escalate
- Creating a practical and effective periodic review process

Best Business Practice Document Included:

☑ Best business practice document for credit, transactional underwriting, documenting over-limit activity, performing periodic reviews and reporting high risk activity to the board of directors or designated committee.

Who Should Attend?

- Account Officers
- Relationship Managers
- Treasury Managers
- Payments Professionals
- Electronic Banking Management/Staff
- Deposit Operations Management/Staff

- Risk Management
- Internal Auditors
- Compliance Management/Staff
- Senior Management

Date: March 11, 2019
Time: 2:00 – 3:00 p.m. EST

Best Business Practices for Defining Risk in Auditing Banks: Since 2009, regulatory fees have dramatically increased, and regulatory consent orders are on the rise. This webinar will focus on best business practices for defining risks in your financial institution. What are the real risks in financial institutions? What is the consequence of not identifying risks? What is a control and what is a risk? Listen to the speaker go through how to effectively and efficiently define the risks throughout all business lines throughout your financial institution.

Topics covered:

- Look at how one department identified 5 major risk categories that most risks statements will fall into,
- helping to identify the "consequence" if the risk is not mitigated.
- Identify the difference between an absence of a control and a risk.

Who Should Attend?

- Internal Auditors
- Risk Managers
- Compliance Officers
- Senior Management
- Legal Staff

Date: March 15, 2018
Time: Noon – 1:00 p.m. EST

Fraud and Ethics: Internal Audit Case Studies: This session will focus on the fraud theory and triangle. What is the fraud triangle and how should that apply to your internal audit focus? This session will also cover real life fraud examples from on auditor's career and how ethics played a role in the fraud. Understand the concept of compliance and its relationship to a healthy ethical culture and legal and regulatory reasons for how you should maintain an effective compliance and ethics program. Also, this webinar will detail how to outline the board's and management's responsibilities for the organization's compliance and ethics program.

Topics covered:

- Defining the Fraud Triangle and Fraud Theory
- Case studies for identifying fraud.
- Understanding how ethics fit into fraud.
- Identification of Senior Management and Board of Director's responsibilities

Who Should Attend?

- Internal Auditors
- Risk Managers
- Compliance Officers
- Senior Management
- Legal Staff

Date: March 15, 2018
Time: 2:00 – 3:00 p.m. EST

Regulation E Compliance, Debit Card Disputes, ACH Unauthorized, Remittance Transfers, Stop Payments and RegTech: How Financial Institutions are complying with Regulation E while improving their efficiencies and risk management - Debit Card disputes, ATM Disputes, ACH Unauthorized, Remittance Transfers and Stop Payments are an integral part of a financial institutions requirements to comply with Regulation E. This hour and a half deep dive webinar will go through each type of error resolution and simplify the process. What is the financial institutions responsibility for complying? How many days do you have to provide provisional credit? How long do you have to perform the investigation for debit cards? What is consumers obligation? What is the timeframe for closing the investigation? How can I make my dispute process more efficient and effective? Financial institutions often struggle with understanding all the dispute deadlines, which letters are required to be distributed to the consumer, when to close out a dispute investigation and all while making their program efficient and effective. This webinar will break down the Regulation E requirement, simplify the process from beginning to end and provide best business practices for significantly enhancing your Regulation E process through industry leading practices including regulatory technology,

Topics include:

- A debrief of Regulation E
- Detailed review of notification, documentation and investigation timeframes for Debit Cards, ACH, ATM, Remittance Transfer and Stop Payments
- What questions are necessary to ask consumers and businesses when a Debit Card dispute has been initiated;
- Effectively communicating to the consumer/business when it is too late to claim an error;
- An overview of how regulatory technology can significantly improve the financial institutions ability to comply and efficiently improve front line and back office debit card dispute workflows

Best Business Practice Document Included:

☑ This webinar will include a frequently asked Regulation E document and a best business practice document for how financial institutions can use RegTechs for Regulation E error resolution investigations workflow.

Who Should Attend?

- Branch Management/Client Facing Teams
- Electronic Banking Management/Staff
- Call Center Management
- Deposit Operations Management/Staff

- Risk Management
- Compliance Management/Staff
- Internal Auditors
- Efficiency Management Officers
- Senior Management

Date: March 26, 2019
Time: 2:00 – 3:30 p.m. EST

ACH Exception Processing for ODFI/RDFI: Complying with the Rules Effectively and Efficiently – Exception processing is a liability for ACH participants – both on the originating and receiving end of the transaction. This webinar will cover ODFI exception processing and Rules requirements such as reversals, returns, notifications of change, reinitiation of return entries, authorization requests and other liabilities. The receiving financial institution (RDFI) also has liabilities when handling exception items including returns, notifications of change, handling unauthorized items, and other liabilities based on network *Rules* and Regulation E. Learn about exceptions as it applies to your daily responsibilities and how you can enhance the effectiveness and efficiencies of your exception item process.

Topics include:
- ODFI Exception Processing and Best Business Practices
- RDFI Exception Processing and Best Business Practices
- Enhancements on ODFI and RDFI Side to improve exception efficiencies

Who Should Attend?
- Client Facing Management/Staff
- Electronic Banking Management/Staff
- Any staff handling Regulation E claims
- Treasury Management
- Client Call Centers
- Internal Auditors
- Risk Managers
- Deposit Operations
- Senior Management

Date: April 2, 2019
Time: 2:00 – 3:00 p.m. EST

Using Data Analytics for Improving Your Internal Audit: Data is important and for internal auditors is a significant indicator of risks. The most difficult piece of having data is knowing how to use it to achieve a well-defined purpose or objective in your internal audit program. How have internal auditors moved to using data analytics to improve their audit and to help financial institutions understand their overall risks and key risk indicators.

Topics Covered:

- How data analytic tools are used.
- Defines opportunities to utilize data analytics in the internal audit work.
- Real life examples of getting started with data analytics.

Who Should Attend?

- Internal Auditors
- Risk Managers
- Compliance Officers
- Senior Management
- Legal Staff

Date: April 10, 2018
Time: Noon – 1:00 p.m. EST

Building Key Performance Indicator (KPI) Dashboards for the Audit Committee: Key performance indicators are an important factor in knowing the effectiveness of your internal audit program. This session focuses on using key performance indicators for Board of Directors to have better visibility into the effectiveness of the internal audit program.

Topics covered:

- IIA Standards give general guidance on what to report to the Audit Committee.
- With the limited time Committee members have, how do you get your performance across in a concise yet accurate format?
- What should be reported?
- What do Committee members need to know beyond the Standards requirements?

Who Should Attend?

- Internal Auditors
- Risk Managers
- Compliance Officers
- Senior Management
- Legal Staff

Date: April 10, 2018
Time: 2:00 – 3:00 p.m. EST

Regulation E Error Resolution Training for Front-Line Staff: Asking the Right Questions and Effectively Handling the Investigation. - Regulation E is often the most confusing regulation for the front line to understand; however, it is a regulation that is critical for complying with consumer laws and regulation. This webinar will go through each type of question that should be asked by the front line when taking error resolution requests and provide client facing staff with a best business practice document with the types of questions that are critical in gathering the right information to complete the investigation. This webinar will also review practical mitigating tools to implement for providing a

positive customer experience while obtaining the right information to successfully closeout a timely error resolution investigation.

Topics covered:

- Overview of Regulation E;
- Review of ACH, Debit Card, and ATM Disputes and Stop Payments
- Error resolution policy and procedures
- Notice of error requirements
- Questions to ask upon notification of an error
- Consumers obligation for timely notification

Best Business Practice Document Included:

☑ Best business practice document with a list of questions to ask for ACH, Debit Card, ATM and Stop Payment Disputes.

Who Should Attend?

- Retail Management
- Deposit Operations
- Regulation E Investigators
- Enterprise Risk Officers
- Risk Managers
- Compliance Officers
- Internal Audit Staff
- Senior Management

Date: April 16, 2019
Time: 2:00 – 3:00 p.m. EST

Traditional and Online Account Opening: Differences, Similarities and Managing Your Risks - The account opening process for consumer and commercial clients creates risk exposure to any financial institution and can be damaging from a risk management perspective. This online training seminar for both Front Line Staff and Managers, as well as Support Staff (Auditors, Risk Analysts, IT/Online Managers, etc.) focuses on the traditional account opening process compared to opening accounts in an online environment.

Topics include:

- A side-by-side comparison of the traditional vs. online account opening environment
- Procedures for traditional versus online account opening
- Review of inherent risks of offering online account opening and compliance requirements for the online account opening environment.
- Top 5 risks that banks and credit unions encounter for both methods
- Lessons learned from online account opening that you'll want to consider when offering the online account opening service

Best Business Practice Document Included:

☑ This webinar will include a risk management comparison chart to use as a quick reference guide.

Who Should Attend?

- Product Management
- Customer Facing Staff
- Internal Auditors
- Compliance Officers
- Risk Managers
- Product Management
- Senior Management

Date: May 14, 2019
Time: 2:00 – 3:00 p.m. EST

Performing a GAP Analysis on Your ACH and Wire Transfer Programs - The FFIEC requires that financial institutions manage the risks associated with using the ACH and wire transfer networks to transmit retail and wholesale payments. Over the past several years, there have been significant risks associated with a financial institutions internal control environment for ACH and Wire Transfers based on significant rules changes, fraud threats, and the evolving payments industry.

Topics include:

- The most prevalent ACH and Wire Transfer risks
- Best business practices for documenting a gap analysis to identify possible gaps in the ACH and Wire programs that could present significant monetary losses and reputational value of the financial institutions brand
- Sample action plan for resolving gaps and how to effectively document the gaps based on regulatory requirements and expectations

Who Should Attend?

- Compliance Officers
- Risk Managers
- Internal Auditors
- Electronic Banking
- Deposit Operations
- Branch Management
- Senior Management

Date: May 23, 2019
Time: 2:00 – 3:00 p.m. EST

Effectively Managing and Overseeing the Risks Associated with Your Remote Deposit Capture Program - Remote Deposit Capture just like other payment collection systems includes guidance, laws and rules that are required for a financial institution to mitigate the risks and ensure compliance with its RDC Program. This webinar will cover FFIEC Guidance on remote deposit capture and take attendees through all applicable risks and provide guidance on how to effectively and efficiently implement risk management controls to mitigate those risks.

Topics include:

- FFIEC Guidance, rules, laws and regulations
- Understanding the Difference between each type of RDC including (Teller Capture, Branch Capture, Mobile Capture, Merchant Capture, Consumer Capture and ATM Capture)
- Knowing the difference between exposure limits and velocity limits
- Effectively managing exceptions such as over-limits, operational issues, technology failures, etc.
- Knowing the most important Key Risk Indicators and Key Performance Indicators to report to your designated committee or Board of Directors
- Best business practices for training your front-line, back-office, and your customers on effectively using RDC to improve risk management efforts within your financial institution

Who Should Attend?

- Compliance Officers
- Risk Managers
- Internal Auditors
- Electronic Banking
- Deposit Operations
- Branch Management
- Senior Management

Date: June 6, 2019
Time: 2:00 – 3:00 p.m. EST

Documenting Your Elder Financial Exploitation Policy: This webinar will focus on regulatory expectations for the implementation of an Elder Financial Exploitation Policy. This session will review each recommended section of the program document, discuss what other policies/procedures are applicable to the Elder Financial Exploitation program, and discuss how to handle exception events that fall outside of the standard process and present higher risk situations for your financial institution and your employees. Attendees will receive a sample Elder Financial Exploitation Program document and the webinar recording to pass along to other employees at your financial institution.

Topics Covered:

- Elder Financial Exploitation
- Components needed in your Elder Financial Exploitation Policy
- Regulatory Guidance and Expectations

Best Business Practice Document

☑ Sample Elder Financial Exploitation Policy Document

Who Should Attend?

- Internal Auditors
- Compliance Officers
- Risk Managers
- Deposit Operations
- Branch Management

- Senior Management

Date: June 13, 2019
Time: 2:00 – 3:00 p.m. EST

Cybercrime Trends and Incident Response Training: The level of inherent cyber security risk varies significantly across financial institutions; however, regulatory scrutiny has significantly increased as cyber-attacks have become a standard course of business for fraudsters and a normal occurrence among financial institutions and companies. Cybercrime has become an advanced persistent threat as the country's financial infrastructure is so dependent upon electronically based internet systems. This webinar will focus on the threats, the FFIEC Guidance which is the minimal guidance for financial institutions to comply, effective payment fraud mitigation controls and the importance of incident response plans.

Topics covered:
- Reviewing the Threat
- Defining Cybercrime
- Review of FFIEC Guidance on Cybersecurity
- Cybercrime trends impacting your payments programs
- Regulatory Requirements and Expectations
- The Importance of Having the Right Insurance Coverage
- Best business practices for mitigating Cybercrime
- Best business practices for documenting your incident response plan

Who Should Attend?
- Fraud Management Staff
- Payments Professionals
- Compliance Management/Staff
- Electronic Banking Management/Staff
- Internal Auditors
- Risk Managers
- Deposit Operations Management/Staff
- Senior Management

Date: July 10, 2019
Time: 2:00 – 3:00 p.m. EST

Wire Transfer Fraud – Prevention, Identification, Escalation, and Recovery: This session will focus on the escalated industry concerns of wire transfer fraud, common wire fraud trends and those trends that are hitting financial institutions that you may not be as prepared to handle today. This session will provide leading business practices on how to effectively build out different workflows to mitigate wire transfer fraud risk, quickly identify a fraud event sooner in the fraud chain, how to handle escalations based on limited amount of time to stop the fraud and the most important recovery steps to have documented before a fraud event occurs. This session will include a leading practice document for quick reference on prevention, identification, escalation and recovery for your front line

and back office staff and a webinar recording to pass along to other employees at your financial institution.

Topics include:

- Wire fraud trends
- Workflows for identification and prevention
- Leading practices for recovering wire transfer fraud

Who Should Attend?

- Fraud Management Staff
- Payments Professionals
- Compliance Management/Staff
- Electronic Banking Management/Staff
- Internal Auditors
- Risk Managers
- Deposit Operations Management/Staff
- Senior Management

Best Business Practice Document Included:

☑ Best Business Practice Document on Wire Transfer Prevention, Identification, Escalation and Recovery Document for Customer Facing and Back-Office Staff

Date: July 25, 2019
Time: 2:00 – 3:00 p.m. EST

Faster Payments and Liquidity Risks: What's the Big Deal for Financial Institutions? The speed at which a payment can be moved is a very hot topic today in the U.S. as many countries have already moved to a faster payment environment. The faster payments movement centers around creating a modern-day system based on the needs of companies and individuals to move money faster and see transactional information as part of the transaction. These risks include the potential inability of banks to measure their liquidity risks in ensuring their payments are appropriately collateralized. This is extremely important for those financial institution moving to a faster payments model (e.g. real-time payments model). The benefits of the customer experience are significant; however, the risks could be significant if the right controls are not in place. This webinar will focus on the faster payments initiative and take attendees through areas of liquidity risks that they should consider if moving to a faster payments' environment.

Topics include:

☑ Brief overview of the Faster Payments Initiatives
☑ Understanding your Payments Exposure
☑ Reporting requirements for Payments Exposure
☑ Consideration if you use a Correspondent Financial Institution for Settlement
☑ Continuity risks between Processing and Finance areas of the Financial Institution

Who Should Attend?

- Financial Institution Finance Departments

- Financial Institution Accounting Departments
- Compliance Management/Staff
- Electronic Banking Management/Staff
- Internal Auditors
- Risk Managers
- Deposit Operations Management/Staff
- Senior Management

Date: August 8, 2019
Time: 2:00 – 3:00 p.m. EST

Deposit Operations Fraud Identification and Prevention: Implementing Fraud Management in the Back-Office: The deposit operations department is an area within each financial institution that may be misunderstood by many as having significant value for identifying fraud. Financial institutions may be missing the opportunity to identify fraud earlier in the risk management chain if deposit operations do not have the appropriate fraud management structure for identifying fraud. This webinar will focus on those areas of fraud risk mitigation controls that can be built into the deposit operations department for preventing and identifying fraudulent activities.

Topics include red flags and suggested procedures for identifying and preventing fraud on:

- Dormant accounts;
- Debit Cards
- New Accounts
- Telephone Transfers
- Changes to Account
- Other Blind Spot areas in Deposit Operations

Best Business Practice Document

☑ Best Business Practice Document for Identifying fraud in Deposit Operations.

Who Should Attend?
- Deposit Operations Management and Staff
- Compliance Officers
- Electronic Banking Management/Staff
- Internal Auditors
- Risk Managers
- Deposit Operations Management/Staff
- Senior Management

Date: August 21, 2019
Time: 2:00 – 3:00 p.m. EST

The Dependency on Mobile Devices to Move Payments: Understanding Mobile Fraud and How to Mitigate the Risks when offering Mobile Services: Mobile banking has grown significantly and so many consumers and businesses depend on their mobile device for information and moving funds.

With the many different methods used for moving funds, the dependency on mobile devices is a significant risk. This webinar will focus on mobile banking fraud threats, fraud events, and what a financial institution should incorporate into its risk management strategy for the use of mobile devices.

Topics include:

- Fraud trends in mobile usage
- FFIEC guidance on the use of Mobile Devices for Banking
- Fraud mitigation controls for using the Mobile Device for Banking
- Effective education for consumers and businesses
- Regulatory expectations for testing the effectiveness of your Mobile Banking risk controls

Best Business Practice Document Included:

☑ Sample Educational Document for your Consumers and Businesses to protect their Mobile Device.

Who Should Attend?

- Information Security Management/Staff
- Information Technology Management/Staff
- Compliance Management/Staff
- Electronic Banking Management/Staff
- Internal Auditors
- Risk Managers
- Deposit Operations Management/Staff
- Senior Management

Date: September 10, 2019
Time: 2:00 – 3:00 p.m. EST

Leading Practices for Documenting Your BSA High-Risk Reviews and Onsite Visits: A significant BSA regulatory requirement is performing high risk reviews. The purpose of high-risk reviews is to ensure that the financial institution has identified, recognized the risks and documented the aggregated risks associated with the continuation of a high-risk customer. This webinar will take attendees through a detailed review of how high-risk reviews should be performed, leading practices on what should be included in the high-risk review and how the financial institutions should incorporate the physical onsite visits into the overall review of such high-risk reviews.

Topics include:

- Background information relating to the high-risk customer
- FFIEC guidelines for determining high risk customers
- FinCEN expectations for high-risk reviews
- Important components to include in your high-risk reviews;
- Common regulatory findings in high-risk reviews;
- Recent enforcement actions addressing weak high-risk programs
- Leading business practices for performing and tracking ongoing high-risk reviews.

Who Should Attend?

- Front line BSA/AML Staff
- Account Opening Staff
- Risk Managers
- BSA/AML Officers
- Compliance Officers
- BSA/AML Audit Staff
- Auditors
- BSA/AML Consultants

Date: September 26, 2019
Time: 2:00 – 3:00 p.m. EST

My Regulator Requires a BSA Model Validation: What is this and Why is it Important? BSA Officers are beginning to hear about the requirement to complete a BSA Model Validation on their BSA Program. Although model validation has been around for years, the trending of regulatory requirements for performing BSA Model Validation has increased over the past few years based on increased BSA consent orders and the need to understand the effectiveness of your BSA program. This webinar will focus on the importance of knowing the significance of performing such validation, what type of information will be requested during the validation, what to expect, and how to select a qualified vendor for performing such review.

Topics include:

- Defining BSA Model Validation
- Regulatory Requirements and Expectations
- Difference between BSA Model Validation and Data Validation
- Components of BSA Model Validation
- Secondary Testing to implement for testing ongoing effectiveness of your BSA Program
- Important Guidance for Selecting a BSA Model Validation service provider

Who Should Attend?

- BSA/AML Officers
- BSA/AML Audit Staff
- Account Opening Staff
- Risk Managers
- Compliance Officers
- Internal Auditors

Date: October 2, 2019
Time: 2:00 – 3:00 p.m. EST

Best Business Practices for Determining Your BSA Customer Risk Scoring Model: From Account Opening Throughout the Duration of the Relationship: BSA risk scoring is an important control for ensuring that the risk profile for your customer base is appropriately scored based on the inherent nature of the customer risk and the residual nature of that customer risk based on various factors.

The risk scoring should be manageable, practical and effectively represent the risks associated with your total customer base to ensure that ongoing enhanced due diligence is performed accurately and timely based on the associated risks with each high-risk customer. This webinar will take attendees through the purpose of risk scoring, implementation of leading business practices for scoring your customer base, and regulatory expectations for reviewing and enhancing these risk scores.

Topics include:

- Defining Customer Risk Scoring
- Regulatory Requirements and Expectations
- Difference between Inherent Risk Scoring and Residual Risk Scoring
- Implementation of Procedures for Changing/Enhancing Risk Scoring
- Important Guidance when changing your risk scoring methodology
- Procedures to include in your BSA Program on risk scoring

Who Should Attend?

- BSA/AML Officers
- BSA/AML Audit Staff
- Account Opening Staff
- Risk Managers
- Compliance Officers
- Internal Auditors

Date: October 22, 2019
Time: 2:00 – 3:00 p.m. EST

Garnishments, Levies and Subpoenas Training for Your Front Line and Back Office: A Practical Guide for Complying with Regulatory Guidance, Federal and State Law: This webinar will cover the legal difference between a subpoena, levy and garnishment and walk attendees through each type of legal request, review a financial institutions customers right to privacy and provide each step a financial institution should follow when receiving, processing, completing and documenting garnishments, levies and subpoenas.

Topics include:

- Regulatory Requirements for Complying and Right to Financial Privacy Act
- Sample procedures for handling Garnishments, Levies and Subpoenas for your Back-Office and Front-Line Staff
- Verifying customer information when complying with subpoenas, garnishments and levies
- Difference in procedures when following Federal vs. State Garnishments;
- Handling IRS Tax Levies
- Understanding when to communicate vs. when not to communicate the receipt of a garnishment, levy, and subpoena

Best Business Practice Document Included:

- ✓ Frequently Asked Questions for Garnishments, Levies and Subpoenas for Financial Institutions
- ✓ A short training deck for training your front-line and back-office when receiving a legal request.

Who Should Attend?

- Risk Managers
- Operations Managers
- Front-Line Staff
- Back-Office Staff
- Compliance Managers
- Internal Auditors
- Senior Management
- Legal Staff

Date: November 13, 2019
Time: 2:00 – 3:00 p.m. EST

Identifying, Preventing and Recovering from Debit Card Fraud: From Internal Controls to Incident Response: Debit card fraud is not always identified based on the customer notification but a great deal of it is identified on the front-line, back-office and through fraud system identification. This webinar will focus on debit card fraud trends, take attendees through each type of debit card fraud event and teach attendees how to identify these types of fraud events based on internal controls including daily functions and system identification. As debit card fraud and breaches can be significant for a financial institution, it is important to understand how to mitigate the risks before the loss is significant. Learn the most effective mitigation tools for identifying debit card fraud before your customer even notifies you and how to implement an effective incident response plan for this type of fraud.

Topics include:

- Debit card fraud trends
- Identification of debit card fraud
- Effective internal controls
- Debit Card Incident Response for Breaches and Significant Fraud Events

Best Business Practice Document Included:

☑ Best business practice document for Debit Card Fraud Mitigating Tools and Incident Response.

Who Should Attend?

- Branch Staff/Client Facing Staff
- Back-Office Staff
- Fraud Managers
- Risk Managers
- Operations Managers
- Compliance/Risk Management
- Internal Auditors
- Legal Staff

Date: December 4, 2019
Time: 2:00 – 3:00 p.m. EST

NEW: COMPLIANCE TRAINING FOR MSBs

Money Service Business (MSB) Annual Required Training for MSBs and Financial Institutions Wishing to Certify the Completion of Their MSBs Training. As defined by FFIEC Guidance, A Money Service Business is generally any person offering check cashing; foreign currency exchange services; or selling money orders, travelers' checks or pre-paid access (formerly stored value) products; for an amount greater than $1,000 per person, per day, in one or more transactions. Money Service Businesses are required by law to comply with all the pillars of BSA including having a compliance officer, effective internal controls, complying with beneficial ownership and control requirements, having an independent audit and ensuring that the MSB is appropriately trained. These requirements are minimum requirements for financial institutions to bank an MSB. This webinar was designed to ensure their MSBs are appropriately trained based on financial institution expectations and includes all regulatory requirements and includes a comprehensive test after the webinar to test the MSBs knowledge. MSBs will receive a certification of completion and the successful passing of the MSB test. This program was designed by a certified AML expert and designed with the understanding of financial institutions general expectations for compliance. Financial institutions' may elect to also receive the certification of completion by their MSB.

Topics include:

- Defining MSB and MSB Activities
- MSB Regulatory Requirements;
- Financial institutions general risk management expectations.
- Leading business practices for ensuring the MSB has a sustainable MSB Program;
- A 5-question exam at the end of the webinar to tests the MSBs knowledge.

Who Should Attend?

- Money Service Businesses
- Financial Institutions offering MSB Services
- BSA/AML Officers
- BSA/AML Audit Staff
- Account Opening Staff
- Risk Managers
- Compliance Officers
- Internal Auditors

This webinar is pre-recorded and includes a five-question test. Once the attendee registers, an attendee link will be sent, and the attendee will be ready to complete the training and take the MSB Compliance test. Attendees will receive a certificate upon completion of the training and successfully passing the MSB test.