



Virginia Bankers Association Internal Audit Seminar

October 4 & 5, 2021



Agenda

Day 1

- Introduction
- Auditing Electronic Funds Transfer
- Auditing the Deposit Function
- Auditing the Branch Operations Function

Day 2

- Pandemic Regulatory Guidance Considerations
- FDICIA/SOx Compliance
- PPP Loan Forgiveness
- Recent Trends in Financial Institution Fraud



Introduction

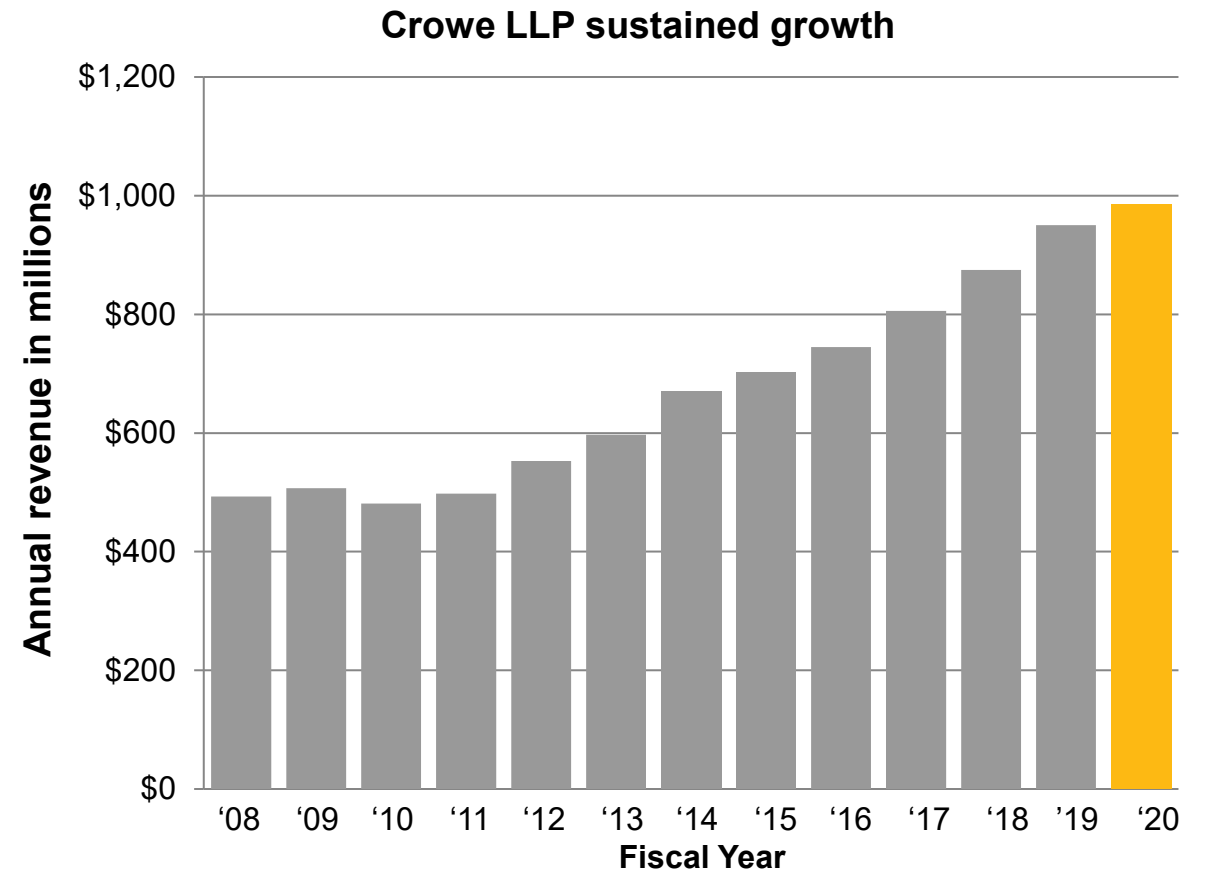


A Little About the Class

- Name
- Bank/Company/Regulatory Agency
- Asset Size/Client Base
- Years in Banking
- Years in Auditing/Security/Compliance
- Your Objective for Class
- Something FUN about YOU
- Favorite Food
- Favorite Book/Movie
- Birthday (Month and Day)

Sustained growth and stability

- Founded in 1942, Crowe is celebrating nearly 80 years of stability, growth, and innovation.
- Crowe ranks as the ninth-largest national accounting firm based on U.S. net revenue.¹
- Crowe Global ranks as the eighth-largest international accounting network.²



¹ The 2020 Accounting Today Top 100 Firms list

² International Accounting Bulletin, 2020, based on market share and fee data

Exceptional client experience

- Crowe uses a best-in-class experience management platform to monitor the experiences we deliver to clients. In the most recent fiscal year:*

97% Said that given the choice, they would do business with Crowe again

96% Said they would recommend Crowe to a colleague

95% Said they really like doing business with Crowe

94% Said Crowe helps them make smart decisions



* Nearly 2,000 completed client surveys

Crowe Knows Banking

- Working with more than 2/3rds of the top 100 U.S. banks
- Performing more U.S. bank holding company audits than any other firm
- Our risk consulting services are endorsed by the American Bankers Association
- Maintaining relationships with more than 400 financial institutions for more than 10 years, and 50 banks for more than 20 years
- Keeping 9 out of 10 Crowe banking specialists with us – and our clients – from year to year.

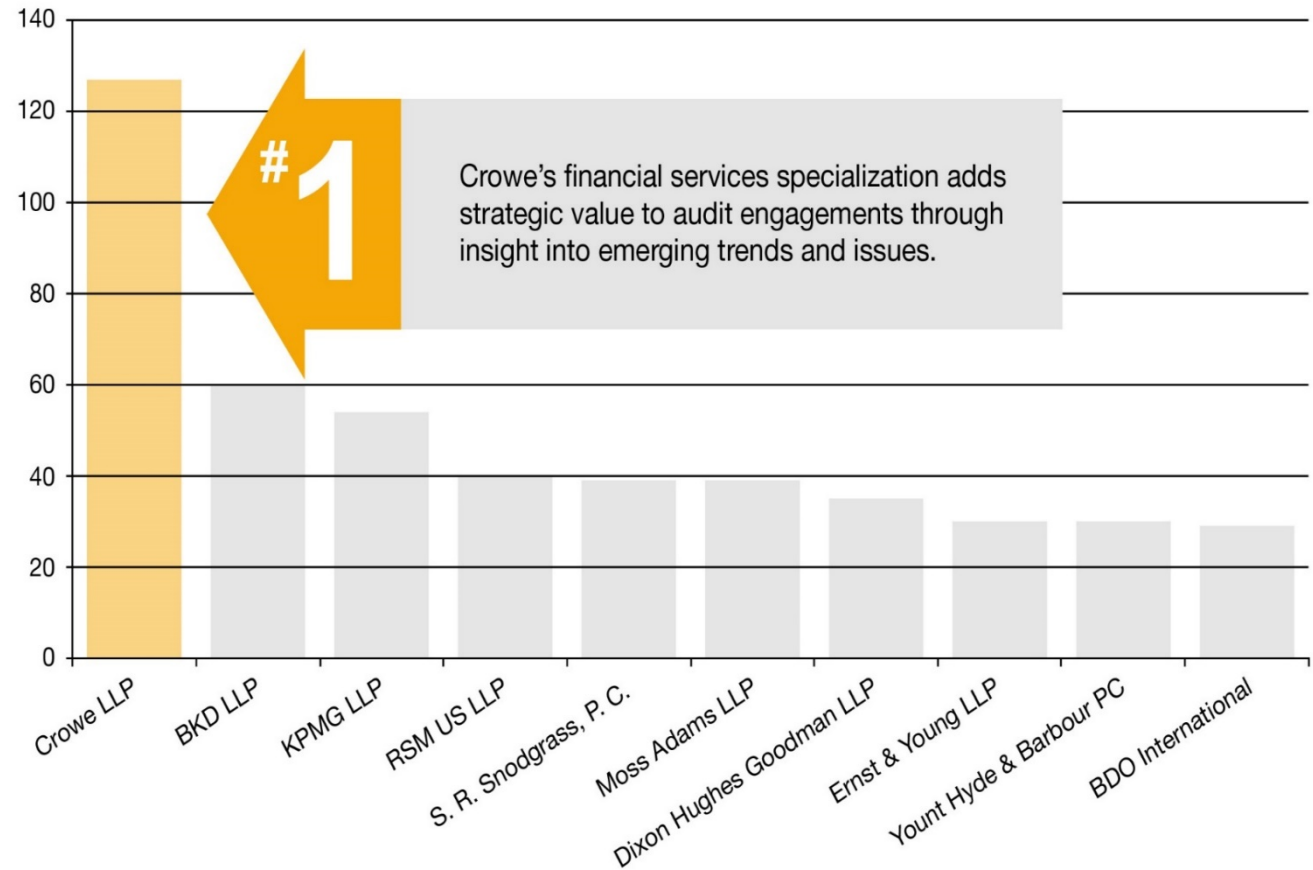


2/3^{rds}
Of the top 100
U.S. banks

400⁺ relationships
maintained

Audit value through industry specialization

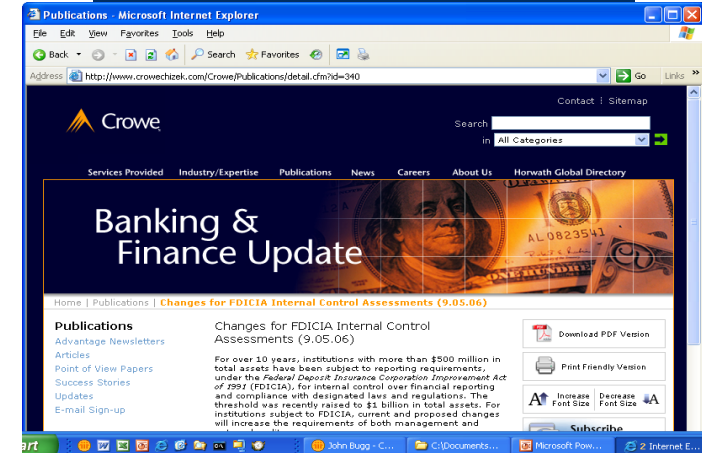
- Crowe ranks No. 1 nationally in the number of audits for publicly traded financial institutions.*



* Source: S&P Global — Marketing Intelligence; August 2020

Crowe Financial Institutions Group

- Crowe publishes timely industry information on critical topics such as accounting issues, tax updates, compliance and bank performance
- Visit www.crowe.com/emailSignup to register for banking e-communications
- Crowe sends periodic invitations for online learning events
- Crowe's Annual Financial Institution Client Conference
- We also provide a number of online resource centers for areas of special interest such as AML/BSA



Crowe's e-Communications

Crowe Financial Institutions Group

- Crowe's Financial Institution Group works 100% of its time with financial institutions
 - Outstanding customer service is critical to your industry – Crowe reflects your commitment by **helping clients succeed**
 - Our **project management focused** audit approach
 - Our **use of technology to streamline the audit**
 - Our **Client Service Standards** set high expectations for our audit teams to deliver client satisfaction
 - Our commitment to **complete our work on time**
 - We audit our performance by **asking for your feedback** through our Client Engagement Survey and other processes

Crowe Financial Services Offerings

We strive for nothing less than a trusted relationship in which every client feels valued:

Audit

Assurance

- Financial statement audits
- Foreign statutory audit
- Benefit plan audits
- IT assurance reporting, including SOC, PCI, and HITRUST
- Reviews, compilations, and other specialized audits

Accounting advisory

- Transaction reporting
- Financial reporting
- IPO readiness

Tax

- Federal tax
- State tax
 - Income tax
 - State and use tax
 - Property tax
 - Credits and incentives
- Washington National Tax
- International tax
- Private client services

Advisory

- Transaction services
- Valuation services
- Performance improvement
 - Operational excellence
 - Strategic sourcing
 - M&A optimization
- Conflict minerals compliance
- Forensic technology and investigation services
- IT advisory
- Restructuring advisory
- Bankruptcy and insolvency services

Consulting

We use deep specialization, technology, and empathy to solve business problems in the following sectors:

- Internal audit
- AML and sanctions
- Independent monitoring
- Third-party risk management
- Enterprise risk management
- Regulatory and compliance services
- Cybersecurity
- Organizational change

Endorsed by the American Bankers Association

Credit Services: outsourced credit review, managing commercial real estate concentrations, credit administration process reviews, ALLL consulting, exam preparation and more.

Internal Audit Services: internal audit outsourcing, Sarbanes-Oxley Act section 404 and FDICIA related testing, audit committee assessment / training and enterprise risk management.

Information Technology Services: IT risk assessments, general controls review in accordance with Federal Financial Institutions Examination Council guidance, security architecture assessment, Gramm-Leach-Bliley Act 501(b) assessment, business continuity planning, ATM pin security (TG3) and more.

BSA / AML Compliance: BSA audits, risk assessments (AML/BSA/Office of Foreign Assets Control), compliance reviews, exam preparation and management, customer risk rating and customer due diligence, Forensic/third party look-backs, board of directors and senior management training and awareness and more.

Regulatory Compliance Services: Regulatory compliance risk assessments, consumer compliance testing, consulting and training, and enterprise-wide compliance risk management, trust operations and administrative reviews, exam preparation and more.



Crowe governance, risk, and compliance management solutions are endorsed by the American Bankers Association (ABA). The ABA endorsement of these solutions indicates they deliver high quality and meet performance standards, and offer the potential to improve your bank's profitability and performance.



Auditing Electronic Funds Transfer

Presented by Edden Burshtein



Agenda

- Wire Transfer
- Automated Clearing House (ACH)
- Internet Banking
- Remote Deposit Capture
- Mobile Banking
- NACHA Rules Updates



Polling Question #1

How comfortable are you when it comes to conducting audits over electronic funds transfer?

- A. Very comfortable
- B. Fairly comfortable
- C. Only slightly comfortable
- D. What is electronic funds transfer?



Wire Transfer

Commercial Account Setup & Monitoring

Essential Control Points

- Wire transfer agreements outline the individuals who are authorized to originate wires on behalf of the customer, their transaction limits, and procedures to be used by the institution to authenticate the transaction, including the identity of the person originating the wire.
- Repetitive wire template set-up is reviewed by a person independent of the original set-up.
- Commercial account system set-up is reviewed by a person independent of the original entry.
- Commercial customers originating wires are required to have a signed agreement on file.

Program Steps

Discuss with management the commercial customer agreement process, including the set-up of the customer on the wire transfer system, repetitive wire transfer template set-up, and the establishment of PINs.

Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation. Select a customer agreement and walk through the set-up process.



Commercial Account Setup & Monitoring

Essential Control Points

- Wire transfer agreements outline the individuals who are authorized to originate wires on behalf of the customer, their transaction limits, and procedures to be used by the institution to authenticate the transaction, including the identity of the person originating the wire.
- Commercial customers originating wires are required to have a signed agreement on file.

Program Steps

Select a sample of commercial customers with agreements and determine whether the agreements designate individuals authorized to originate wires as well as required signatures.



Commercial Account Setup & Monitoring

Essential Control Points

- Commercial account system set-up is reviewed by a person independent of the original entry.
- Commercial customers originating wires are required to have a signed agreement on file.

Program Steps

Select a sample of new commercial customer set up reports and determine whether an independent review of the input to the system was performed.



Commercial Account Setup & Monitoring

Essential Control Points

- Repetitive wire template set-up is reviewed by a person independent of the original set-up.

Program Steps

Select a sample of new repetitive template set up reports and determine whether an independent review of the input to the system was performed.

Commercial Account Setup & Monitoring

Essential Control Points

- An agreement exists with the correspondent bank used to process wire transfer transactions. The agreements outline the individuals who are authorized to originate wires, their transaction limits, and procedures to be used by the institution to authenticate the transaction, including the identity of the person originating the wire.

Program Steps

Discuss with management the correspondent agreement process as it relates to wire transfer. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

Obtain the current correspondent agreements for which wire transfer activity is processed through. Determine whether authorized individuals listed on the agreements are currently employed by the institution

Incoming Wire Processing

Essential Control Points

- Incoming wires are accurately and timely posted to accounts and fees are assessed according to the institution's fee schedule.
- Incoming wire transfer advices are maintained.

Program Steps

- Discuss with management the incoming wire transfer process, from receipt of wire transfer advice to recording on the system and general ledger. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Select an incoming wire and walk through the process.
- Select a sample of incoming wire transfers and determine the following:
 1. the wire amount (including fees) posted to the customer account agrees to the advice;
 2. the wire amount posted to the correspondent bank account agrees to the advice;
 3. the wire was posted on the same business day as the advice was received;
 4. The fees charged agree to the institution's fee schedule.

Outgoing Wire Processing

Essential Control Points

- Outgoing wires are processed with collected funds or with daylight overdrafts approved by institution employees with adequate authority.
- The authenticity and authority of the originator is verified.
- Outgoing wires are accurately and timely posted to accounts and fees are assessed according to the institution's fee schedule.
- Outgoing wire transfer requests are documented and approved by authorized account users.
- Wire transfer requests received via telephone are recorded.
- Telephone requests are only accepted for those customers who have wire transfer agreements and assigned PINs/test codes.
- Outgoing wires are verified by an individual not responsible for input of the wire.
- Outgoing wire transfer requests are approved by bank employees with adequate wire transfer authority.

Program Steps

Discuss with management the outgoing wire transfer process, from receipt of wire transfer request to recording on the system and general ledger. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation. Select an outgoing wire and walk through the process.

Outgoing Wire Processing

Program Steps

Select a sample of outgoing wire transfers and determine the following:

1. the request was documented on a wire transfer form;
2. the form was signed by the customer or authorized by the customer through the use of a PIN/test key/test code;
3. the customer's signature or identity was validated by institution personnel;
4. the requestor is an authorized user on the account the wire is drawn on;
5. phone requests are only accepted for those customers who have signed agreements;
6. collected funds were on deposit to fund the wire or if collected funds were not on file, the daylight overdraft was properly approved;
7. the wire was approved by an institution employee with adequate wire transfer authority;
8. the wire was verified by person who did not input the wire;
9. if required by the agreement, callback procedures were performed;
10. if the wire request was received via telephone and institution procedures require it, the request was recorded;
11. the correct amount (including fees) was properly posted on the correct day to the customer and correspondent account;
12. the fees charged agree to the institution's fee schedule.

Outgoing Wire Procedures

Essential Control Points

- Written procedures exist and describe the critical processes and controls within this activity.

Program Steps

Assess the following for the procedures related to this activity:

1. Existence: Do procedures exist for this activity? If not, should the institution have them?
2. Current: Are procedures a reflection of current practice and controls?
3. Completeness: Are procedures complete with respect to critical elements of the activity and the critical control points?

Outgoing Wire Balancing

Essential Control Points

Incoming and outgoing wire transfer activity is balanced by an independent party on a daily basis. Out of balance conditions are resolved by individual independent of the balancing function.

Program Steps

- Discuss with management the wire transfer daily balancing process. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Select a sample of daily balancing of wire transfer activity and determine whether the activity is balanced independent of the processing of wires and total dollars and number of wires sent and received is reconciled between the request forms/incoming advices and the wire transfer system.

Outgoing Wire Safeguarding

Essential Control Points

- Wire transfer documentation (agreements, request forms, PIN lists, test codes, test keys) is secured and access is restricted.
- The institution has established insurance and fidelity bonds, including loss of records coverage, in order to protect the institution from potential loss resulting from wire transfer transactions.
- Workspace access, layout, and conditions provide restricted access.
- An annual assessment is performed and consultation with insurers is performed to determine coverage is adequate. The institution's risk manager maintains insurance policies.
- Background checks, credit checks and drug screens have been performed for employees moving into the wire transfer function.

Program Steps

Discuss with management the process of safeguarding of assets as it relates to wire transfer. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.



Outgoing Wire Safeguarding

Essential Control Points

- The institution has established insurance and fidelity bonds, including loss of records coverage, in order to protect the institution from potential loss resulting from wire transfer transactions.
- An annual assessment is performed and consultation with insurers is performed to determine coverage is adequate. The institution's risk manager maintains insurance policies.

Program Steps

Determine whether management has performed an annual assessment of the adequacy of insurance and fidelity bonds. Obtain evidence of the review.



Automated Clearing House

ACH Process

Typically, there are five parties to an ACH transaction:

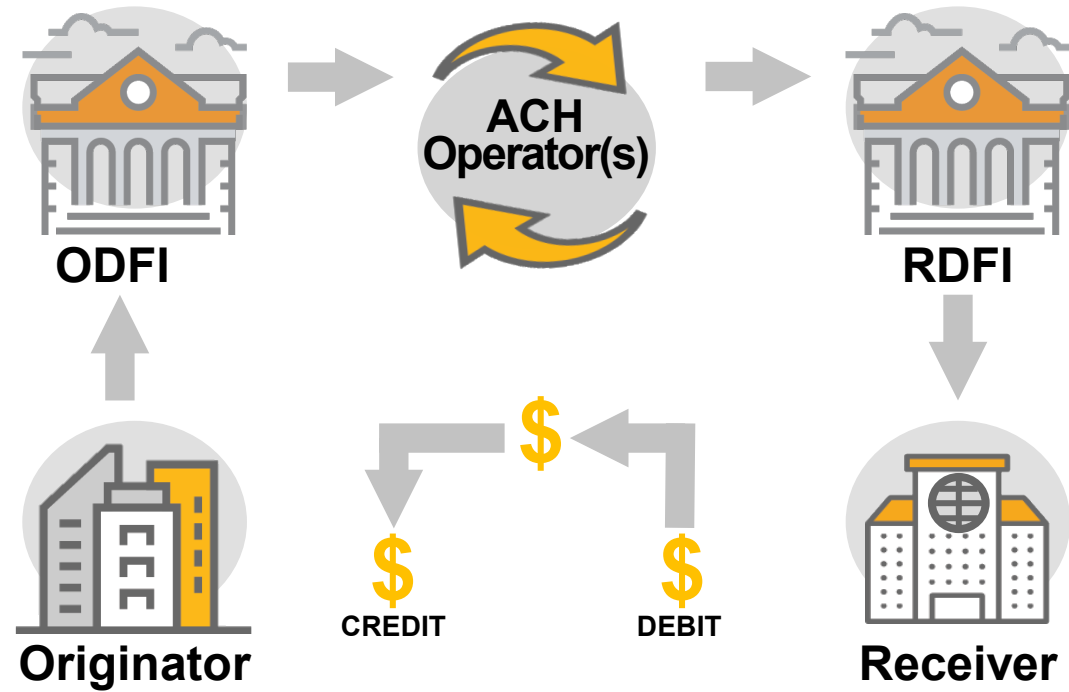
1. The originator, either an organization or an individual
2. The originating depository financial institution (ODFI)
3. The ACH operator, a private organization, or a U.S. Federal Reserve Bank (FRB), which serves as a central clearing facility through which financial institutions transmit or receive ACH entries
4. The receiving depository financial institution (RDFI)
5. The receiver, an individual, or an organization that has authorized an originator to initiate an ACH entry to its account

Polling Question #2

What does “ACH” stand for?

- A. Automated Clearing House
- B. Automotive Clearing House
- C. Automatically Clean House
- D. No clue!

ACH Process



Source: www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html

RDFI – Correspondent Account Setup & Monitoring

Essential Control Points

An agreement exists with the correspondent bank used to process ACH transactions. The signed agreements outline the individuals who are authorized to process ACH transactions.

Program Steps

- Discuss with management the correspondent agreement process as it relates to ACH. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Obtain the current correspondent agreements for which ACH activity is processed. Determine whether authorized individuals listed on the agreements are currently employed by the institution.



RDFI – Procedures Assessment

Essential Control Points

Written procedures exist and describe the critical processes and controls within this activity.

Program Steps

Assess the following related to procedures in the area:

1. Existence: Do procedures exist for this process? If not, should the institution have them?
2. Current: Are procedures a reflection of current practice and controls?
3. Completeness: Are procedures complete with respect to critical elements of the process and the critical control points

RDFI – Processing

Essential Control Points

- Customer information is verified prior to entries being returned.
- An individual independent of processing received ACH files reviews all rejects and/or exceptions.
- Received ACH files are balanced daily by an individual independent of the processing function.
- Required documentation is obtained for customer originated ACH return transactions.
- Originated return transactions and notifications of change information are returned to the originator and information is transmitted to the originator on a timely basis.
- The financial institution's ACH system parameters are set so that transactions are automatically posted to customer accounts on settlement date, not effective date, and funds are made available to customers on settlement date.

Program Steps

Discuss with management the processing of received ACH files, from receipt of the file to recording on the system and general ledger as well as the balancing process and debits that overdraw the customer's account. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.



RDFI – Processing

Essential Control Points

Received ACH files are balanced daily by an individual independent of the processing function.

Program Steps

Select a sample of balancing work for received files. Trace batch totals to the correspondent bank account. Determine whether a person independent of the daily processing is responsible for performing the balancing.



ODFI – Procedures Assessment

Essential Control Points

Written procedures exist and describe the critical processes and controls within this activity.

Program Steps

Assess the following for the procedures related to this activity:

1. Existence: Do procedures exist for this process? If not, should the institution have them?
2. Current: Are procedures a reflection of current practice and controls?
3. Completeness: Are procedures complete with respect to critical elements of the process and the critical control points?

ODFI – Processing

Essential Control Points

- Independent verification of originated ACH files is performed prior to the file being released.
- Originator's exposure limits are reviewed prior to the file being released and originated files that exceed the customer's exposure limits are approved by an institution employee with adequate authority prior to being released.
- Originated ACH files are balanced daily by an individual independent of the processing function.
- Customer authorizations are obtained prior to reinstatement of ACH originated return entries.
- Personal identification numbers (PINs) or other positive identification methods are used for originated ACH transactions.
- An individual independent of processing originated ACH files reviews all rejects and/or exceptions.
- A system or manual "pre-funding" process is in place to debit the customer's account or to verify the account balance prior to releasing an originated credit file. For high-risk businesses, the financial institution withholds a pre-set percentage of the debit entry file for a pre-set number of days against the risk of returned transactions.
- The financial institution monitors the ACH activity of its originators for rules violations, TEL and WEB activity, and for unauthorized returns.

Program Steps

Discuss with management the processing of originated ACH files, from receipt of the file and verification of exposure limits to recording on the system and general ledger as well as the balancing process. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation. Select an originated file and walk through the process to substantiate your understanding.



ODFI – Processing

Essential Control Points

Originated ACH files are balanced daily by an individual independent of the processing function.

Program Steps

Select a sample of balancing work for originated files. Trace batch totals to the correspondent bank account. Determine whether a person independent of the daily processing is responsible for performing the balancing.

ODFI – Originator Setup & Monitoring

Essential Control Points

- An independent review of new originator system set-up is performed.
- An annual review of exposure limits is performed for all originators, changes to the limits are communicated to management and the system is updated to reflect the change.
- Internal ACH transfer limits for employees who originate transactions have been established and a process is in place to approve transfers that exceed the established limits.
- ACH Originators are required to have an agreement on file.
- Individuals have been assigned the responsibility of approving ACH credit exposure limits for ACH originators.
- “Per day” and “per file” exposure limits have been established for each originator. The exposure limits are noted in the customer agreement and entered in the system. Originators are approved by an authorized individual with sufficient unsecured credit authority and in accordance with the financial institution's ACH underwriting standards.

Program Steps

Discuss with management the process of approving, setting up and monitoring ACH originators, including the review of the customer's creditworthiness, setting of initial exposure limits, and the annual review of exposure limits. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation. Select an originator and walk through the approval and set-up process.

ODFI – Originator Setup & Monitoring

Essential Control Points

- An independent review of new originator system set-up is performed.
- ACH Originators are required to have an agreement on file.
- Individuals have been assigned the responsibility of approving ACH credit exposure limits for ACH originators.
- “Per day” and “per file” exposure limits have been established for each originator. The exposure limits are noted in the customer agreement and entered in the system.

Program Steps

Select a sample of originators to determine the following:

1. An independent review of the set-up was performed.
2. An agreement is on file for each.
3. Per day and per file exposure limits have been established by an authorized institution employee.
4. Agree approved exposure limits in the agreement to the ACH system.



ODFI – Originator Setup & Monitoring

Essential Control Points

- An annual review of exposure limits is performed for all originators, changes to the limits are communicated to management and the system is updated to reflect the change.
- “Per day” and “per file” exposure limits have been established for each originator. The exposure limits are noted in the customer agreement and entered in the system.

Program Steps

Select a sample of originators that have been submitting files for over a year. Determine if an annual exposure limit review was performed, the ACH system was updated, and the new limits were communicated to applicable management.

ODFI – Originator Setup & Monitoring

Essential Control Points

ACH Originators are required to have an agreement on file.

Program Steps

Obtain a copy of the current ACH origination agreement and determine whether it contains the following:

1. Security procedures for the transmission of entries
2. Provisional credit disclosure
3. Individuals authorized to send files
4. Procedures for handling rejected entries
5. Fee and data retention and processing schedules
6. A dollar limit for transfers requested by authorized individuals
7. Call back procedures for files over an authorized individuals limit
8. Originations on uncollected funds - states they are not allowed unless approved by an officer with lending authority to do so
9. Hold requirements for funds
10. Accounts for settlement of funds

ODFI – Third-party Origination

Essential Control Points

- The client of the third-party processor signs an agreement that includes an assumption of financial liability for files that are submitted on their behalf. The third-party processor has signed an agreement that includes an assumption of responsibility for compliance with NACHA requirements for files that it submits on behalf of its clients.
- The credit of the client of the third-party processor is reviewed. A "per day" limit is approved by an individual with sufficient unsecured lending authority.
- The client of the third-party processor is set up on the ACH system with the approved “per day” limit.
- The account of the client of the third-party processor is debited for files that the third-party submits on their behalf.
- The client of the third-party processor is a customer of the institution.

ODFI – Third-party Origination

Program Steps

Discuss with management the process of entering into a relationship with a third-party processor and their clients. Consider the following issues:

- What agreement does the institution use when a client agrees to assume liability for the files that are submitted by the third-party on their behalf?
- Does this agreement specifically address the third-party relationship?
- Does the agreement have specific language that says the client of the third-party will assume financial liability for files submitted on their behalf?
- Who is assigned to review the client's credit?
- Does this individual have sufficient unsecured loan authority to approve the credit limit?
- What financial and credit records are reviewed?
- Is the review documented and retained?
- Is the client a customer of the institution?

Discuss the process of set-up of a new client of the third-party on the ACH system, including the "per day" limit and the account that is debited for the submitted files. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

ODFI – Third-party Origination

Program Steps

Obtain a list of all of the third-party relationships and a list of their clients. Determine if the third-party relationship is "sender" or "processor". For all of the third-party processors, determine the following:

- There is an agreement on file that includes the appropriate language of assumption of financial liability by the client of the third-party processor.
- The agreement has been signed by the client and by the institution.
- The account of the client is debited for submitted files.
- The client's credit has been reviewed/approved. The review has been documented and the documentation has been retained.
- A "per day" limit is set for the client and the "per day" limit is input into the system.
- The client is a customer of the institution.
- The third-party processor has signed a different agreement that includes an assumption of responsibility for compliance with NACHA requirements for files that it submits on behalf of its clients.



ODFI – Third-party Origination

Essential Control Points

- The third-party sender has signed an agreement that includes an assumption of financial liability and an assumption of responsibility for compliance with NACHA requirements for files that it submits on behalf of its clients.
- The third-party sender's account is debited for files that it submits on behalf of its clients.
- The third party sender's credit is reviewed/approved for the total exposure of all of its clients. A "per day" limit is assigned for the third-party sender by an individual with sufficient unsecured lending authority.
- The third-party sender is set up on the ACH system with the approved "per day" limit.

ODFI – Third-party Origination

Program Steps

Discuss with management the process of entering into a relationship with a third-party sender who will submit files for its clients. Consider the following issues:

- Who is assigned to review the third-party's credit? Does this individual have sufficient unsecured loan authority to approve the credit limit? What financial records are reviewed? Is the review documented and retained?
- What agreement does the institution use when a third-party agrees to assume liability for the files that it submits on behalf of its clients? Does this agreement specifically address a third-party relationship? Does the agreement have specific language that says the third-party will assume financial liability for files submitted?
- Discuss the process of set-up of a new third-party on the ACH system, including the "per day" limit and the account that is debited for the submitted files.

Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

ODFI – Third-party Origination

Program Steps

Obtain a list of all of the third-party relationships. Determine if the third-party relationship is "sender" or "processor". For all of the third-party senders, determine the following:

- There is an agreement on file that includes the appropriate language of assumption of financial liability by the third-party.
- The agreement has been signed by the third-party and by the institution.
- The account of the third-party is debited for submitted files.
- The third-party's credit has been reviewed/approved for the total exposure of all of its clients. The review has been documented and the documentation has been retained.
- The individual who approved the "per day" limit has sufficient unsecured loan authority.
- A "per day" limit is set for the third-party and the "per day" limit is input into the system. Refer to Guidance for more information.

ACH Exercise

You are the Audit Manager and you are reviewing the below workpaper completed by the Junior Auditor.

After reviewing the workpaper, get into your groups and discuss the following:

- Do you agree with the Junior Auditor's conclusion?
If yes, why? If no, why?
- What information, if any, on the workpaper is a basis for concern?
If so, what is the concern?
- What, if any, additional procedures might you perform?

After reviewing the above questions, discuss in your groups recent trends you are seeing in your bank relative to ACH processing.



Internet Banking

Internet Banking Operations

Essential Control Points

- Written policies have been drafted which address all internet banking functions.
- Authorization is obtained during set up of all internet banking accounts.

Program Steps

- Obtain the policies and procedures related to internet banking. Observe whether the policies and procedures address significant aspects of internet banking functions. The policies and procedures should include basic internet access setup with and without bill payment services, customer verification, password requirements, file maintenance, reconciliation of accounts, documentation retention, commercial ACH and EFTPS transactions, vendor management, internal controls, system access, and contingency plan.
- Select a sample of accounts signed up for Internet Banking and obtain the signed authorization and approval for the account activation.
- Inquire with management regarding the activation of accounts for access through Internet Banking. Specifically address: signed request for activation by the customer, ability to transfer funds between accounts with different owners, maintenance performed on accounts, authorization for bill payment services, documented credit checks for activation to initiate ACH debits.



Internet Banking Operations

Essential Control Points

- Appropriate individuals are assigned responsibility and authority for processing internet transactions.

Program Steps

Through discussion with management, observation during a walkthrough of the function, and review of policies and procedures, gain a comprehensive understanding of the bank's internet banking function. Document in narrative and flowchart form all controls in place and identify any weaknesses identified. Document employee duties for internet banking, the bank's core processing system, and any other bank system. Determine that duties are adequately segregated throughout the function.

Internet Banking Operations

Essential Control Points

- File maintenance changes are restricted to authorized individuals.
- File maintenance changes are reviewed in a timely manner by supervisory personnel who are not involved in executing the changes. Unusual or specific changes are compared to supporting documents.

Program Steps

- Through inquiry, determine the procedures for making master file changes for internet banking accounts. Determine whether changes are made by an employee without account access and that changes are independently reviewed. Determine if employees performing file maintenance for internet bank accounts also perform file maintenance on the bank's core processing system. Determine that duties are adequately segregated throughout the function.
- Identify a sample of customer initiated master file changes made by the Call Center. Trace to evidence that proper documentation is maintained to support customer authorization.
- Select a sample of maintenance changes from the change log and trace the change to a signed authorization document.



Internet Banking Operations

Essential Control Points

- Negotiable items are adequately safeguarded to prevent theft and wrongful use.
- Access/ ability to process customer check orders is restricted to authorized individuals.

Program Steps

- Discuss procedures for processing customer check orders and information changes, such as address, name on check, and account numbers. Ensure duties are properly segregated and that orders are independently reviewed.
- Review physical controls over unused drafts.
- Determine that customers' checks are shipped independent of the employee processing the check order. Determine whether orders returned as undeliverable are received independent of the employee processing the orders.

Internet Banking Operations

Essential Control Points

- Fees are assessed and collected appropriately.
- Waived fees are approved by appropriate management and routinely monitored.

Program Steps

- Discuss procedures for waiving fees. Determine that management is reviewing waivers and identifying lost income.
- Discuss the fee structure for access to Internet Banking and review associated income accounts for reasonableness of the fees collected. If fees are commonly waived, discuss the reasons for waiving the fees and procedures followed. Determine if customers' accounts are specifically coded to waive fees during an introductory period. Walkthrough the procedures for ensuring the customer's account code is changed and charged fees after the introductory period has expired.
- Review deposit service charges on employee and officer accounts to determine whether service charges are similar to other depositors, including criteria for waived charges.



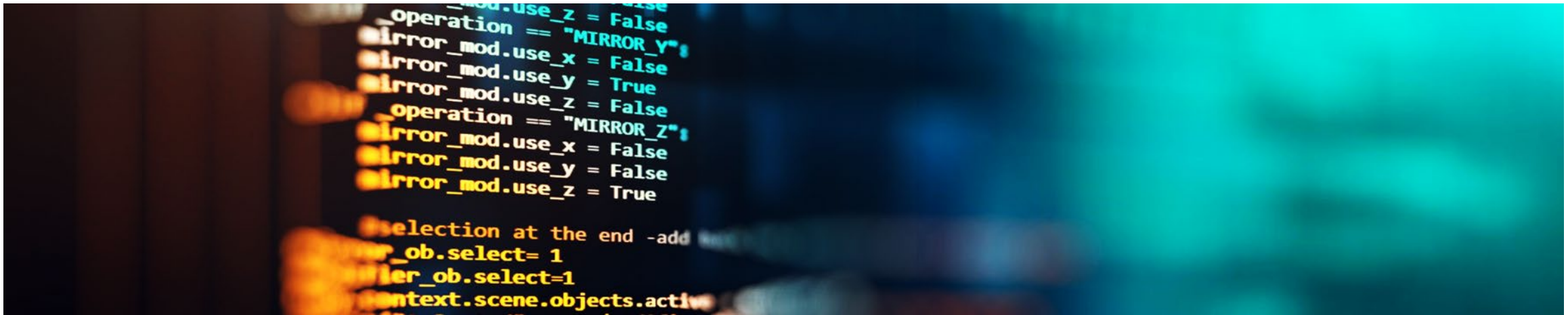
Internet Banking Operations

Essential Control Points

- New account responsibilities are appropriately restricted.
- Employee accounts are adequately evaluated and approved prior to set up.

Program Steps

- Identify a sample of new accounts opened by the Call Center. Observe whether proper identification was obtained and if all documentation was properly prepared.
- Review procedures followed during the process of opening, setting up, and approving employee and officer internet banking deposit accounts.



Remote Deposit Capture

Origination & Processing – Branch Capture

Essential Control Points

- As items are scanned, the remote capture software encodes items with their item number and batch number.
- The electronic file of the images is encrypted for secure transmission over the internet.
- Image quality rejects are resolved the same day by an authorized individual who is independent of the responsibility of scanning and transmission.
- Original items that were scanned are retained in a secure location and destroyed after a predetermined number of days.
- The remote capture software has duplicate item detection safeguards.
- An end-of-day completeness check is performed, i.e., the branch communicates the total number and total dollar of transmitted items, and the operations center confirms the receipt of those same totals.
- The institution has established back-up procedures in case electronic transmission is not available.
- A quality control review is performed, i.e., reject reports are periodically reviewed by management to identify equipment, software, or employee use problems.
- Access to branch capture software is controlled by authentication security (i.e., User IDs, passwords).

Program Steps

Discuss with management the branch capture process, from software access to the scanning of items, and to the transmission and safekeeping of items. Discuss the related tasks of resolving image quality rejects, end-of-day completeness checks, back-up procedures, and monitoring reject reports. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.



Origination & Processing – Branch Capture

Essential Control Points

An end-of-day completeness check is performed, i.e., the branch communicates the total number and total dollar of transmitted items, and the operations center confirms the receipt of those same totals.

Program Steps

From the current audit cycle, obtain a sample of branch reports that show end-of-day transmission totals. Determine that the branch has retained evidence that an end-of-day completeness check was performed - i.e., the branch has retained an end-of-day totals report and an email or faxed memo from the operations center that confirms the receipt of the same totals. Note: as this testing entails obtaining documentation from the branches, the in-charge may decide to perform testing during the branch audits.



Origination & Processing – Branch Capture

Essential Control Points

As items are scanned, the remote capture software encodes items with their item number and batch number.

Program Steps

From the current audit cycle, select a sample of items and review for evidence the items are encoded with an item number and batch number. Trace to final item processing reports to determine if items can be readily identified for future research efforts.



Origination & Processing – Branch Capture

Essential Control Points

The remote capture software has duplicate item detection safeguards.

Program Steps

From the current audit cycle, for a sample of days, review reports for evidence the remote capture software identifies and reports possible duplicate items.



Origination & Processing – Branch Capture

Essential Control Points

A quality control review is performed, i.e., reject reports are periodically reviewed by management to identify equipment, software, or employee use problems.

Program Steps

From the current audit cycle, obtain management's most recent quality control review and determine if management is monitoring for possible equipment, software, or user problems. If a problem is identified, discuss with management the steps taken to resolve the problems.

Origination & Processing – Commercial & Consumer Capture

Essential Control Points

- The customer's remote capture software has duplicate item detection safeguards.
- The electronic file of the images is encrypted for secure transmission over the internet.
- The remote capture software has limited micr modification, i.e., it limits what data the depositor can change after the check is scanned.
- Access to customer remote capture software is controlled by multi-factor authentication security.
- The institution requires the customer to retain the original items in a secure location and destroy them after a predetermined number of days.

Program Steps

Discuss with management the process of capturing and transmitting the customer's deposit, from software access to the scanning of items, and to the transmission and safekeeping of items. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.



Origination & Processing – Commercial & Consumer Capture

Essential Control Points

The customer's remote capture software has duplicate item detection safeguards.

Program Steps

From the current audit cycle, for a sample of days, review reports for evidence the remote capture software identifies and reports possible duplicate items.



Origination & Processing – Commercial & Consumer Capture

Essential Control Points

The remote capture software has limited micro modification, i.e., it limits what data the depositor can change after the check is scanned.

Program Steps

From the current audit cycle, for a sample of customers and days, review system reports for evidence that changes to MICR information are identified and management has reviewed such changes for accuracy and appropriateness.



Origination & Processing – Commercial & Consumer Capture

Essential Control Points

- Customers are approved for remote capture by an authorized individual in accordance with the institution's acceptance criteria.
- “Per deposit” and “per day” remote deposit limits have been established for customer accounts by an authorized individual.
- Signed agreements are on file for each customer who submits deposits via remote capture and the agreement outlines key components.

Program Steps

Discuss with management the process of approving new customers for remote deposit capture. Comment on the institution's acceptance criteria and the individual assigned responsibility for approving customers. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

Origination & Processing – Commercial & Consumer Capture

Essential Control Points

Signed agreements are on file for each customer who submits deposits via remote capture and the agreement outlines key components.

Program Steps

Obtain a copy of the current customer agreement for remote capture. Determine that the agreement addresses the following:

- image quality
- must be adequate and meet the bank's requirements
- "per deposit" limits, "per day" limits
- warranties against duplicate presentment, alterations, forged maker or forged endorsement signatures, losses, viruses, compliance with applicable laws, etc.
- liability for the retention, security, and destruction of original items. Items should be destroyed after a pre-set number of days. Retention should be long enough for availability for problem resolution and for maker's dispute, yet short enough to prevent duplicate presentment.
- item eligibility
- i.e., no foreign items [not eligible per Check 21 law], no items with red ink, no items over a certain dollar amount, no third-party checks, no checks drawn on the customer or its affiliates (defense against check kiting)- hardware and software standards
- rejects and error resolution, lost/stolen items, and funds availability
- acceptance/rejection of files
- the Bank is not obligated to accept a file; it is subject to provisional credit
- disclosure of fees
- which state laws govern the transactions

Origination & Processing – Commercial & Consumer Capture

Essential Control Points

- Customers are approved for remote capture by an authorized individual in accordance with the institution's acceptance criteria.
- “Per deposit” and “per day” remote deposit limits have been established for customer accounts by an authorized individual.
- Signed agreements are on file for each customer who submits deposits via remote capture and the agreement outlines key components.

Program Steps

From the total population of commercial and consumer customers who submit deposits via remote capture, select a sample of customers who were added during the current audit cycle. Review the files and agreements for the following attributes: - A signed agreement is on file. - The agreement or file shows evidence of approval by an authorized individual. - The agreement lists the customer's "per deposit" and "per day" limits. - If the operations center software monitors "per deposit" and "per day" limits, obtain screen prints of the customer's limits on the system and agree the limits on the agreement to the limits on the system.

Origination & Processing – Pre-Posting Review

Essential Control Points

- Deposits that are over the customer's “per day” or “per deposit” limits are detected and rejected before posting.
- The processing of deposits that violate “per deposit” or “per day” limits require prior approval by an authorized individual or over-limit deposits are held for next day processing. Customer deposits and branch batches are “proved” (credits equal debits) by the remote capture software before transmission or by the institution's processing software before posting.
- Items not drawn on a US institution are identified, and the original items are forwarded to the Fed in a timely manner by an individual who is independent of capture and transmission.
- Before posting, the system detects and rejects items and deposits that have previously been presented.
- Image quality analysis is performed by the remote capture software before transmission or by the institution's processing software before posting to the customer’s account.
- Rejected and returned items, over-limit violations, and image quality analysis reports are periodically reviewed by management to monitor customer compliance with the terms of the agreement.
- Dollar thresholds have been established over which images are flagged for bank review of endorsements, check stock, valid payee, and evidence of alterations. Out-of-balance deposits are identified and resolved in a timely manner by authorized personnel independent of the responsibility of transmission.
- If original items are not required to be forwarded to the institution, back-up files of the images are maintained.
- The institution has fraud detection software that reviews remote capture transactions for suspicious activity, i.e., check stock verification, check numbers out of sync, duplicate check numbers, new account activity.



Origination & Processing – Pre-Posting Review

Program Steps

Discuss with management the process of reviewing remote capture branch items and customer deposits before posting and submission to the Fed. Discuss the detection of limit violations, balancing and correcting transactions, submitting foreign items, monitoring customer rejects, reviewing items over thresholds for fraud. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

Origination & Processing – Pre-Posting Review

Essential Control Points

- Deposits that are over the customer's “per day” or “per deposit” limits are detected and rejected before posting.
- The processing of deposits that violate “per deposit” or “per day” limits require prior approval by an authorized individual or over-limit deposits are held for next day processing. Customer deposits and branch batches are “proved” (credits equal debits) by the remote capture software before transmission or by the institution's processing software before posting.

Program Steps

Obtain a sample of system reports from the current audit cycle that list "per day" and "per file" limit violations. Determine if there is evidence of review (i.e., the report is initialed). Determine if there is evidence of research and response to limit violations - i.e., the deposit is held for next day processing or there is evidence of approval by an authorized individual for processing. Note: this step may not be applicable if the detection and prevention of "per-day" or "per file" limit violations is controlled by the front-end software - i.e., the depositor is unable to submit a file over his file limit or over his daily limit.



Origination & Processing – Pre-Posting Review

Essential Control Points

Dollar thresholds have been established over which images are flagged for bank review of endorsements, check stock, valid payee, and evidence of alterations.

Program Steps

Obtain a sample of remote capture reports from the current audit cycle that list items over the institution's review threshold. Determine if there is evidence of review of the items - i.e., the report is initialed by the individual who reviewed the items. Determine if there is evidence of research and response to any suspicious items - i.e., there are notes on the report that indicate the account was frozen or documentation was retained that shows the maker was contacted.



Origination & Processing – Pre-Posting Review

Essential Control Points

Before posting, the system detects and rejects items and deposits that have previously been presented.

Program Steps

Obtain a sample of remote capture reports from the current audit cycle that list items and/or deposits that have previously been presented. Determine if there is evidence of review of the items - i.e., the report is initialed by the individual who reviewed the items. Determine if there is evidence of research and response to the duplicate items or deposits - i.e., the deposit was not posted, the customer was contacted, the account was flagged.

Note: The customer front-end software may prevent duplicate electronic presentment of items from their computer, but it may not prevent the customer from scanning and submitting the check electronically and then bringing the original item to the ATM or to the branch for duplicate credit. Some software will spray "SCANNED" across the front of items as they scan in order to deter duplicate presentment. Duplicate items should be detected before deposits are posted.

Origination & Processing – Pre-Posting Review

Essential Control Points

- Customer deposits and branch batches are “proved” (credits equal debits) by the remote capture software before transmission or by the institution's processing software before posting.
- Out-of-balance deposits are identified and resolved in a timely manner by authorized personnel independent of the responsibility of transmission.

Program Steps

Obtain a sample of remote capture reports from the current audit cycle that list out-of-balance transactions. Determine that there is evidence that the out-of-balance transactions have been resolved - i.e., items are checked off on the report, the report is initialed by the individual who resolved the items. Determine that the individual who resolved the out-of-balance transactions was independent of the transmission of the transaction. Consider testing a sample of items to determine the account was credited or debited for the difference amount. Determine that items were resolved in a timely manner - i.e., the same day. Inquire regarding automatic notification of customer.

Note 1: this program step may not be applicable if the branch and customer front-end software detects and prevents transmission of out-of-balance transactions. **Note 2:** this program step may be covered in the Deposit Operations / Item Processing audit program.



Origination & Processing – Pre-Posting Review

Essential Control Points

Items not drawn on a US institution are identified, and the original items are forwarded to the Fed in a timely manner by an individual who is independent of capture and transmission.

Program Steps

From the current audit cycle, obtain system reports that identify items not drawn on a US institution. For a sample of items, trace to ultimate receipt of funds from the Fed or a correspondent bank. Note: this program step may be covered in the Deposit Operations / Item Processing audit program.



Origination & Processing – Pre-Posting Review

Essential Control Points

Rejected and returned items, over-limit violations, and image quality analysis reports are periodically reviewed by management to monitor customer compliance with the terms of the agreement.

Program Steps

Obtain management's most recent review of customer activity. Determine that customer activity was reviewed for evidence of lack of compliance with the terms of the agreement. Discuss with management the steps taken to resolve the problems. If customers are assessed additional fees for noncompliance, review a sample of client statements for evidence the fees were correctly assessed.

Origination & Processing – Third-party Vendors

Essential Control Points

- The institution performs due diligence prior to the approval of a third-party relationship.
- The institution has a signed agreement on file for each of its third-party relationships and the agreement includes key components such as business recovery, duplicate item detection, and image quality analysis.
- A contingency plan exists in the event a vendor cannot perform as expected.
- Management monitors the internal controls of vendors on a periodic basis.

Program Steps

Discuss with management the processes performed by third-party vendors relating to remote capture. Document the process, considering the essential control points. Also comment on: the pre-posting review performed by the vendor: image quality analysis, duplicate presentment detection, fraud detection - the processing controls: how rejects and out-of-balance transactions are resolved - the signed agreement: does it also include liability and privacy/security clauses? Comment on whether the controls are designed effectively and are in operation.

Origination & Processing – Third-party Vendors

Essential Control Points

- The institution performs due diligence prior to the approval of a third-party relationship.
- The institution has a signed agreement on file for each of its third-party relationships and the agreement includes key components such as business recovery, duplicate item detection, and image quality analysis.

Program Steps

- Obtain a list of the new third-party remote capture relationships for the current audit cycle and determine the following: A signed agreement is on file for each third-party relationship.
- The agreement includes key components: image quality analysis, business recovery, duplicate item detection, fraud detection, privacy/security responsibility, warranties for liabilities, monitoring customer "per day" and "per file" limits, review of items over an established dollar threshold.
- Due diligence was performed prior to the approval of the relationship.



Mobile Banking



Mobile Banking - Governance

Essential Control Point

- The financial institution has created a mobile banking policy and assessed the risks associated with the service.

Program Steps

Determine if the financial institution has developed a Mobile Banking strategy, including a documented Strategic Plan and cost-benefit analysis. Ensure senior management has provided adequate oversight of the Mobile Banking initiative.

Determine if the Management has analyzed the risks associated with new mobile banking services within a risk assessment and that the Board of Directors has reviewed and approved the risk assessment within the last 12 months.



Mobile Banking – Employee Access

Essential Control Point

- There are adequate controls surrounding mobile banking employee access.

Program Steps

Examine procedures and related forms for user accounts which are newly set-up, modified, or deleted to ensure management has a formal process for managing user access.

Obtain a list of new hires and transfers during the last twelve months from the human resources department and determine that the proper procedures and related forms were utilized for the access change.

Obtain a list of all terminations during the last twelve months from the human resources department and determine if user profiles for all terminated employees were properly disabled or deleted.



Mobile Banking – Employee Access

Essential Control Point

- There are adequate controls surrounding mobile banking employee access.

Program Steps


Obtain a list of all users with administrative privileges and determine if the users with access to these accounts are appropriate.

Examine documentation concerning assignment of passwords to note the frequency with which they are changed and note standards for password creation. Obtain a report from the system validating passwords settings are in

accordance with company policy.

Obtain previous security logs to validate management's review process is conducted regularly and is appropriate.

Obtain the results from the most recent user access level review. Evaluate the effectiveness of the review and determine that it is conducted annually.



Mobile Banking – Customer Access

Essential Control Point

- There are adequate controls surrounding mobile banking customer/member access.

Program Steps

Determine that a formal and secure method of adding and modifying Mobile Banking access has been created with proper management approval before account access is granted.

Determine that a formal process exists for deleting Mobile Banking accounts upon account termination.

Determine that customers/members are reviewed and verified before they are granted access to the mobile banking system.

Determine that the Mobile Banking system is protected by strong password parameters that adhere to industry best practice.

Determine that the client has implemented multi-factor authentication to strengthen the security of the Mobile Banking system.

Mobile Banking – Service Providers

Essential Control Point

- Service providers are reviewed to ensure appropriate controls exist to protect the availability, confidentiality, and integrity of customer information.

Program Steps

Determine that the client performs adequate vendor management for the Mobile Banking provider, including an annual review of service provider performance.

Obtain and examine the contract with the Mobile Banking Service Provider (MBSP) to ensure the following terms are included:

1. Restrictions on use of nonpublic customer information collected or stored by the MBSP.
2. Requirements for appropriate controls to protect the security of customer information held by the MBSP.
3. Service-level standards such as website up-time, hyperlink performance, customer service response times.
4. Incident response plans, including notification responsibilities, to respond to website outage, defacement, unauthorized access, or malicious code.

Mobile Banking – Service Providers

Essential Control Point


- Service providers are reviewed to ensure appropriate controls exist to protect the availability, confidentiality, and integrity of customer information.

Program Steps

(Continued from prior Slide.)

Obtain and examine the contract with the Mobile Banking Service Provider (MBSP) to ensure the following terms are included:

5. Business continuity plans for Mobile Banking services including alternate processing lines, backup servers, emergency operating procedures.
6. Limitations on subcontracting of services, either domestically or internationally.
7. Choice of law and jurisdiction for dispute resolution and access to information by the financial institution and its regulators.
8. For foreign-based vendors or service providers (i.e., country of residence is different from that of the institution), in addition to the above items, contract options triggered by increased risks due to adverse economic or political developments in the vendor's or service provider's home country,



Mobile Banking – Service Providers

Essential Control Point

- Service providers are reviewed to ensure appropriate controls exist to protect the availability, confidentiality, and integrity of customer information.

Program Steps

Determine that the client conducts a documented, annual review of the Mobile Banking service provider's SAS 70 report, including an inspection of the report's opinion, control testing exceptions and user control considerations.



National Automated Clearing House Association (NACHA)

NACHA – General

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (Record Retention) and (Electronic Records) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through inquiry and review of the institution's record retention policy, determine whether the DFI or third party provider, if applicable, has retained records of all ACH transactions for a minimum period of six years. (This Includes any manually created documentation (e.g. Written Statements Under Penalty of Perjury). Document the following:</p> <ul style="list-style-type: none"> a. Where retained b. What format <p>Obtain a copy of the record of entries for a date six years from the audit date.</p>	<p>Through discussions, may need to verify if there are any ACH entries sent manually to the ACH Operator (i.e. NOC entries) or if there are any entries processed outside the normal process such as unauthorized entries. Commonly we see Financial Institutions or Credit Unions manually return NOC entries and return unauthorized entries through FedLine which only retains entries for 30 days. See common audit findings.</p> <p>Note: Per Regulation E, WSUDs must be retained for two years from settlement date of the returned entry. This is an additional year longer than what is required under NACHA rules.</p> <p>Operating Rules and Page Reference</p> <ul style="list-style-type: none"> 1.4.1 Retention Requirement for Records of Entries, OR 2 1.4.2 Provision Requirement for Records of Entries, OR 2 1.4.3 Electronic Record Creation and Retention, OR 2

NACHA – General

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (General Audit Requirements) and (Annual Audit Verification) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through inquiry with management and through review of documentation, verify that RDFI has completed the annual audit of compliance with NACHA Rules for the previous calendar year.</p>	<p>If the Financial Institution just started processing ACH entries for Originators during the prior year make sure they completed the ODFI audit requirements as part of their last NACHA audit. See common audit findings.</p> <p>Operating Rules and Page Reference</p> <p>1.2.2 Audit of Rules Compliance, OR 1</p>
	<p>For any findings noted in the previous year, determine that the findings have been addressed and cleared.</p>	

NACHA – General

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules, (ACH Data Security Requirements) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Determine that if the RDFI transmits Financial Institution information by either encrypted or transmitted via a secure session, in either case using a commercially reasonable technology that complies with applicable regulatory requirements. Financial Institution information includes any Entry, routing number, account number, PIN or other identification symbol.</p>	<p>Transmissions of banking information over an Unsecured Electronic Network by means of voice or keypad inputs from a wireline or wireless telephone to a live operator or voice response unit are not subject to this section.</p> <p>Operating Rules and Page Reference</p> <p>1.7 Secure Transmission of ACH Information VIA Unsecured Electronic Networks, OR3</p>

NACHA – General

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (Payment of Annual Fees and Per-Entry Fees) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through inquiry with management and review of payment documentation, determine that the ODFI has paid the network fees as required by NACHA Rules.</p>	<p>An ACH Operator serves as a central clearing facility that receives entries from the Financial Institutions and distributes the entries appropriately to other Financial Institutions. There are currently two ACH Operators: FedACH and Electronic Payments Network (EPN). FedACH is the Federal Reserve Financial Institutions' Automated Clearing House (ACH) service.</p> <p>Note: Most Financial Institutions send their ACH entries through an ACH Operator for processing. The purpose of the inquiry is to identify Financial Institutions that may be sending large volumes of ACH entries directly to another institution and not through an ACH Operator. These Financial Institutions may not be aware they are still required to report and pay the fee to NACHA through filing an N-7 form.</p> <p>Operating Rules and Page Reference</p> <p>1.13 Network Administration Fees, OR 4</p>

NACHA – General

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (Risk Assessment and Risk Management Program), can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Obtain the entity’s most recent risk assessment of the risks of its ACH activities and verify that the risk assessment has been updated periodically (usually annually) and reflects the current environment.</p>	<p>A risk management program is a process where policies, procedures, and controls effectively address all aspects or risk regarding the Financial Institution's ACH activities.</p> <p>If also performing an ACH audit, a good thing to do would be to determine if the risk assessment is updated annually and presented to a committee (i.e. I.T. Steering Committee) for review. This could be documented in an ACH workpaper since it's not a requirement of NACHA.</p> <p>Operating Rules and Page Reference</p> <p>1.2.4 Risk Assessment , OR1</p>

NACHA – General

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (Security Requirements) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Conclude that each non-consumer Originator, Participating DFI and Third-Party Service Provider has established, implemented, and updated, as appropriate, policies, procedures, and systems with respect to the initiation, processing, and storage of Entries that are designed to:</p> <ul style="list-style-type: none"> (a) protect the confidentiality and integrity of Protected Information until its destruction; (b) protect against anticipated threats or hazards to the security or integrity of Protected Information until its destruction; <p>and,</p> <ul style="list-style-type: none"> (c) protect against unauthorized use of Protected Information that could result in substantial harm to a natural person. <p>Such policies, procedures, and systems must include controls that comply with applicable regulatory guidelines on access to all systems used by such non-consumer Originator, Participating DFI, or Third Party Service Provider to initiate, process, and store Entries.</p>	<p>Could discuss where the ACH information is stored (including back-up information) and determine what policies are in place (i.e. Information Security Policies) to protect this information. As data is often stored with vendors the Financial Institution should consider controls the vendor has as part of their vendor risk management program. Also discuss the controls in place - if the Financial Institution minimizes where they save and store information, block potential intruders through use of firewalls and antivirus software and restrict employees who have access to the data.</p> <p>Operating Rules and Page Reference</p> <p>1.6 Security Requirements, OR3</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (RDFI Pre-notification Processing) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through the review of policies and procedures, inquiry and observation of Financial Institution operations personnel, determine the processes management performs to confirm the accuracy of posting of the pre-notifications received, including but not limited to the following:</p> <ol style="list-style-type: none"> Pre-notifications can be clearly identified on daily reports (Example: via transaction codes or pre-notification reports); Upon receipt of pre-notifications, operations personnel verify the accuracy of account number information; If the account indicated by a pre-notification is unidentifiable, a return entry is initiated indicating the account number is invalid (Return reason code R03 or R04); If the account number is incorrect, but the intended account can be identified through the combination of other entry information, a Notification of Change (NOC) entry is initiated to advise the ODFI of the correct account information; Returns and Notifications of Changes are processed in accordance with required deadlines (See timelines below). 	<p>A Prenotification (a.k.a. Prenote) is an optional zero dollar ACH entry that precedes an actual debit or credit entry</p> <p>(Returns and NOCs must be originated no later than the banking day following the settlement date of the pre-notification and NOCs must be initiated within two banking days following the settlement date of the pre-notification)</p> <p>NACHA Rule Book Section 3.5 - Specific Provisions for Pre-notifications, page OR 45</p> <p>Please refer to the Knowledge Library for the corresponding Detailed Testing Spreadsheets.</p> <p>EFFECTIVE 1/2020, Originators will be required to perform supplemental screening related to WEB debit entries to confirm account validation. This could include an increase in prenote transactions or other types of account validation requests. The RDFI's process surrounding prenote verification should be considered with this in mind.</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (RDFI Pre-notification Processing) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Select a sample of control occurrences during the audit period based on the control frequency and the sampling methodology. Revise the initial request item description to align to the needs of the test procedures. Work with your team members to communicate the initial requests to the Client Service Manager or other appropriate client contact.</p>	
	<p>Select a sub-sample of transactions using the documentation obtained for the sample of control occurrences. Save the sample selection in a separate document and revise the sampling request item description to align to the needs of the remaining test steps. Work with your team members to communicate the sampling requests to the Client Service Manager or other appropriate client contact.</p>	
	<p>For each sample selected, determine whether returns or NOCs were initiated by required deadlines.</p>	

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (RDFI Notification Of Change Processing) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through inquiry and observation, document whether the financial institution complies with the following procedures:</p> <ol style="list-style-type: none"> When the financial institution receives an ACH transaction that contains incorrect information, a notification of change (NOC) entry is originated to prevent future items from rejecting; All NOCs, except in cases of mergers and acquisitions, are transmitted to the ACH Operator within two days of the settlement of the original entry; The financial institution verifies the accuracy of the information in the NOC. 	<p>Operating Rules and Page Reference</p> <p>3.9.1 General Rule for Notification of Change (COR Entry), OR 49</p> <p>The Financial Institution may choose not to send Notification of Change (COR) entries to prevent future items from rejecting. Then the Financial Institution must send a return entry for any invalid ACH entries received and since the Financial Institution does not send correction entries this section of testing is not applicable.</p> <p>Subsection 3.9.1 General Rule for Notification of Change (COR Entry)</p> <p>Please refer to the Knowledge Library for the corresponding Detailed Testing Spreadsheets.</p>
	<p>Select a sample of control occurrences during the audit period based on the control frequency and the sampling methodology. Revise the initial request item description to align to the needs of the test procedures. Work with your team members to communicate the initial requests to the Client Service Manager or other appropriate client contact.</p>	
	<p>Select a sub-sample of transactions using the documentation obtained for the sample of control occurrences. Save the sample selection in a separate document and revise the sampling request item description to align to the needs of the remaining test steps. Work with your team members to communicate the sampling requests to the Client Service Manager or other appropriate client contact.</p>	
	<p>Review a sample of NOC entries to determine that the time deadlines have been met.</p>	

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (Acceptance of Entries) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through inquiry, determine whether operations personnel refuse any type of ACH entry (i.e., debits to savings accounts, other debits or reversals).</p>	<p>NACHA Rule Book RDFI Must Accept Entries, OR 40</p> <p>Exceptions to Restrictions on RDFI’s Right to Transmit Return Entries, OR 47</p> <p>Destroyed Check Entries (XCK) are entries originated by an ODFI for collection of certain checks contained in a lost or destroyed cash letter shipment; or checks that cannot be processed through image exchange. The words “NO CHECK” and “CHECK DESTROYED” in the Company Entry Description and Company Name fields, respectively, identify these entries. XCK entries must be accompanied by the serial number of the lost check. This information should appear on the account holder’s periodic statement to help identify the entry. The Financial Institution has the right to decline the acceptance of XCK entries because they are more susceptible to fraud as there is not evidence of authorization (i.e. no check) from the customer.</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (RDFI Returns) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through inquiry with management and review of policies and procedures, determine the manner and timing in which entries that have been refused by the Receiver are returned.</p>	<p>Subsection 3.8.3.2 – Timing Requirements for Credit Entries Refused by Receiver</p>
	<p>Through inquiry with management and review of policies and procedures, determine the manner and timing in which unposted credits are reviewed and either resolved or returned. When returned, determine how the return reason code is assigned and whether the return entries are processed by the ACH Operator's deposit deadline for the Return Entry to be made available to the ODFI no later than the opening of business on the second Banking Day following the Settlement Date of the original Entry.</p>	<p>Subsection 3.8.4 RDFI Must Return Unposted Credit Entries</p> <p>Part 4.2 Table of Return Reason Codes</p> <p>Subsection 3.8.3 Exceptions to Timing Requirements for Return Entries</p>
	<p>Select a sample of control occurrences during the audit period based on the control frequency and the sampling methodology. Revise the initial request item description to align to the needs of the test procedures. Work with your team members to communicate the initial requests to the Client Service Manager or other appropriate client contact.</p>	<p>Subsection 3.8.4 RDFI Must Return Unposted Credit Entries</p>
	<p>Select a sub-sample of transactions using the documentation obtained for the sample of control occurrences. Save the sample selection in a separate document and revise the sampling request item description to align to the needs of the remaining test steps. Work with your team members to communicate the sampling requests to the Client Service Manager or other appropriate client contact.</p>	
	<p>Select a sample of returned entries, other than those returned for stop payments or unauthorized entries, include all other return codes. Determine that the returns were processed in accordance with the proper timelines and the return reason code is accurate based on the type of entry, type of account (consumer/non-consumer), and properly supported. (Note: The sample should include all types of entries (CCD, CTX, PPD, ARC, BOC, etc. to both consumer and non-consumer accounts.)</p>	

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (Credit Availability and Debit Posting) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through review of policies and procedures, inquiry and observation of Financial Institution operations personnel, determine whether:</p> <p>Same Day Credit Entries</p> <p>a) Entries received during the first processing window must be made available to the receiver no later than 1:30 pm RDFI local time.</p> <p>b) Entries received during the second processing window must be made available to the receiver no later than 5:00 pm RDFI local time.</p> <p>Non-Same Day Credit Entries</p> <p>a) Entries made available to the RDFI by the ACH Operator by 5:00 pm on the Banking Day prior to the Settlement Date must be made available to the Receiver for withdrawal no later than 9:00 AM on the Settlement Date.</p> <p>b) Entries made available to the RDFI by the ACH Operator after 5:00 pm on the Banking Day prior to the Settlement Date must be made available to the Receiver for withdrawal by the end of the Settlement Date.</p>	<p>Operating Rules and Page Reference</p> <p>3.3.1 General Rule for Availability of Credits, OR 42</p> <p>3.3.2 Timing of Debit Entries, OR 43</p> <p>EFFECTIVE September 20, 2019</p> <p>Subsection 3.3.1.1 Availability of Credits That Are Not Same Day Entries</p> <p>Subsection 3.3.1.2 Availability of Credits That Are Same Day Entries</p> <p>Same Day Entry Fee</p> <p>The NACHA Operating Rules require each Originating Depository Financial Institution (ODFI) to pay a Same Day Entry Fee to the respective Receiving Depository Financial Institution (RDFI) for each Same Day ACH Entry that is originated by or through the ODFI.</p> <p>The fee received by each RDFI for each Same Day transaction is \$.52</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (Credit Availability and Debit Posting) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Document alternative methods used in the event of an erroneous posting, posting delays or possible rejects or consumer credit entries to ensure timely availability.</p> <p>Select a sample of Same Day entries received and obtain evidence that the entry was posted by the required timeframes:</p> <p>CREDIT ENTRIES ONLY</p> <p>If the entries were received PRIOR to September 19, 2019, determine the entries were made available to the receiver for withdrawal by 5:00 pm on the Settlement Date of the transaction.</p> <p>If the entries were received AFTER September 19, 2019, determine the following:</p> <ul style="list-style-type: none"> a) Entries received during the first processing window were made available for withdrawal by 1:30 pm RDFI local time, b) Entries received during the second processing window were made available for withdrawal by 5:00 om RDFI local time. <p>If the RDFI indicates that no Same Day entries were received, obtain the statements from the ACH Operator for the audit period and determine that there were no "Same Day Entry Fees" being received during this time period.</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (Credit Availability and Debit Posting) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Select a sample of entries that are not Same Day entries and determine the following:</p> <p>DEBIT ENTRIES:</p> <p>The entry must not be posted to the customer's account prior to the Settlement Date even if the Effective Date is different from the Settlement Date.</p> <p>CREDIT ENTRIES:</p> <p>If the entries were received PRIOR to September 19, 2019, determine the following</p> <ol style="list-style-type: none"> a) All entries, except PPD entries, were made available for withdrawal by the consumer by the end of business on the Settlement Date, RDFI local time. b) PPD credit entries received by the RDFI by 5:00 pm on the banking day prior to the settlement date must be made available to the Receiver for withdrawal by the opening of business on the Settlement Date. <p>If the entries were received AFTER September 19, 2019, determine the following:</p> <ol style="list-style-type: none"> a) Entries made available to the RDFI by the ACH Operator by 5:00 pm on the Banking Day prior to the Settlement Date must be made available to the Receiver for withdrawal no later than 9:00 AM on the Settlement Date. b) Entries made available to the RDFI by the ACH Operator after 5:00 pm on the Banking Day prior to the Settlement Date must be made available to the Receiver for withdrawal by the end of the Settlement Date.

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (Credit Availability and Debit Posting) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Select a sample of control occurrences during the audit period based on the control frequency and the sampling methodology. Revise the initial request item description to align to the needs of the test procedures. Work with your team members to communicate the initial requests to the Client Service Manager or other appropriate client contact.</p> <p>Select a sub-sample of transactions using the documentation obtained for the sample of control occurrences. Save the sample selection in a separate document and revise the sampling request item description to align to the needs of the remaining test steps. Work with your team members to communicate the sampling requests to the Client Service Manager or other appropriate client contact.</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (Credit Availability and Debit Posting) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Select ACH transactions from the posting journal for all types of entries (i.e., PPD, CCD, CTX, ARC, POP, RCK, POS, XCK, MTE, SHR, BOC, IAT), compare information to customer account statements and observe whether the statement identifies the following:</p> <ul style="list-style-type: none"> a) Posting date to customer's accounts; b) Dollar amount of the entry; c) Company/Originator name; d) Company entry description; e) Type of account (e.g., checking); f) Number of the account; g) Amount of any charges assessed against the account for electronic fund transfer services;\ h) Balances in the customer's account at the beginning and at the close of the statement; i) For an ARC, BOC, RCK or XCK Entry, or an IAT Entry where the Transaction Type Code field contains a value of "ARC," "BOC," or "RCK," the Check Serial Number; j) For an MTE, POS or SHR Entry, or an IAT Entry where the Transaction Type Code field contains a value of "MTE," "POS," or "SHR," the: <ul style="list-style-type: none"> i. Terminal identification code and/or terminal location, as those terms are defined in Regulation E; ii. Terminal city, as that term is defined in Regulation E; and iii. Terminal state, as that term is defined in Regulation E; k) For a POP Entry, or an IAT Entry where the Transaction Type Code field contains a value of "POP," the: <ul style="list-style-type: none"> i. Check Serial Number; ii. Terminal city, as that term is defined in Regulation E; and iii. Terminal state, as that term is defined in Regulation E; l) Address and telephone number to be used for inquiries or notices of error preceded by "Direct Inquiries To" or similar language m) For RCK Entries, the descriptive information contained in the Entry is included in the periodic statement.

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (Credit Availability and Debit Posting) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Document the method used to originate Returns of ACH Transactions (i.e., FEDLINE, Voice Response, Bulk Data, Data Processor, Correspondent Financial Institution).</p>
	<p>Review existing documentation that verifies the timing of receipt by the ACH Operator of returned debit entries. Document measures taken to verify routing of returns to avoid un-timeliness due to misrouting.</p>
	<p>Determine if the Financial Institution has returned any permissible returns of CCD or CTX entries (i.e., unauthorized debits to non-Consumer Accounts) since the last NACHA Self Audit. If so, review documentation to determine that the return was processed with permission of the ODFI and that the correct Return Code was used. Determine the manner in which the ODFI authority the RDFI to return the item.</p>
	<p>Document procedures followed when a dishonored return entry is received and time deadlines for responding to a dishonored return should the RDFI wish to contest the dishonored return.</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (Credit Availability and Debit Posting) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Select a sample of contested dishonored returns and determine the following:</p> <ul style="list-style-type: none"> a) the original Return Entry was, in fact, returned within the time limits established by these Rules; b) the original Return Entry was not a duplicate Entry; c) the original Return Entry was complete and contained no errors; d) the dishonored Return Entry was misrouted or untimely; e) the dishonored Return Entry relates to an Erroneous Entry or a related Reversing Entry, both of which were previously returned by the RDFI; or f) the funds relating to the R62 dishonored Return Entry are not recoverable from the Receiver (for use ONLY with dishonored Returns R62 – Return of Erroneous or Reversing Debit). <p>The RDFI must Transmit a contested dishonored Return Entry to the ACH Operator within two Banking Days after the Settlement Date of the dishonored Return Entry and must ensure the contested dishonored Return Entry otherwise complies with the requirements of Appendix Four (Return Entries).</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (Credit Availability and Debit Posting) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Document how Re-presented Check entries are identified.</p>
	<p>Document the procedures in place to control the proper handling of Re-presented Check Entries to ensure these are returned by midnight of the second banking day following banking day of receipt of the presentment notice (originally entry).</p>
	<p>Review existing documentation that verifies the timing of receipt by the ACH Operator of returned credit entries. Document measures taken to verify routing of returns to avoid un-timeliness due to misrouting.</p>
	<p>Through discussion with management, determine that all unposted credit entries are returned to the ACH Operator within the same day or next of the settlement date so they able to be made available to the ODFI on the opening on the second banking day.</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (RDFI Minimum Description Standards) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through inquiry with management and review of policy and procedures, determine the following:</p> <ul style="list-style-type: none"> a) The manner and timing in which stop payment requests are accepted and whether the Bank requires such requests to be in writing for consumer accounts (Note: written requests are required for stop payments to non-consumer accounts within 14 days of the verbal request) b) If the Bank requires the verbal stop payment request to be followed with a written request, determine how the Bank discloses this to the customer and the timing of when the verbal stop payment ceases to be binding. c) Whether stop payment requests are accepted on recurring debits and how such requests are documented as opposed to a stop requested on a single entry; d) If stop payment requests are accepted on all future payments of recurring debits, determine whether the Bank requires the customer to state in writing that authorization has been revoked and the manner in which this is documented. <p>Consumer Accounts: Determine whether the stop payment order remains in effect until the earlier of:</p> <ul style="list-style-type: none"> a) the withdrawal of the stop payment order by the Receiver; or b) the return of the debit Entry, or, where a stop payment order applies to more than one debit Entry relating to a specific authorization involving a specific Originator, the return of all such debit Entries. <p>Non-Consumer Accounts: Determine whether the stop payment order remains in effect until the earlier of:</p> <ul style="list-style-type: none"> a) the withdrawal of the stop payment order by the Receiver; b) the return of the debit Entry; or, c) six months from the date of the stop payment order, unless it is renewed in writing. 	<p>Operating Rules and Page Reference</p> <p>3.1.5.1 RDFI Must Provide Entry Information for Consumer Accounts, OR 40;</p> <p>3.1.5.2 RDFI Must Provide Entry Information to Receives of ARC, BOC or POP Entries to Non-Consumer Accounts OR 41</p> <p>Appendix Three ACH Record Format Specification, OR 83</p> <p>Subsection 3.4.5 Specific Warranties for RCK Entries</p> <p>Please refer to the Knowledge Library for the corresponding Detailed Testing Spreadsheets.</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (RDFI Minimum Description Standards) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Document the process in place to identify a check upon which a stop payment has been placed if presented as an ACH transaction.</p> <p>Select a sample of stop payment returns from the return testing reports. Review a sample of initiated stop payment returns to determine the following:</p> <ul style="list-style-type: none"> a) A written stop payment order was obtained for stop payments to non-consumer accounts and as applicable to consumer accounts. b) The transaction to which the entry relates was received AFTER the stop payment request was made by the customer. c) The transaction was returned using the return reason code R08 d) The transaction was returned within two banking days of the settlement date of the transaction. <p>Document the procedures in place for obtaining a completed Written Statement of Unauthorized Debit with respect to any of the following:</p> <ul style="list-style-type: none"> a) unauthorized or improper debit Entry to a Consumer Account; b) unauthorized or improper ARC, BOC, or POP Entry to a Non-Consumer Account; c) unauthorized IAT Entry; d) Incomplete Transaction to a Consumer Account or an Incomplete Transaction involving any ARC, BOC, or POP Entry; and e) Improperly Reinitiated Debit Entry. <p>Determine whether the entries are returned within the appropriate time frames and the appropriate return reason code.</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (RDFI Timely Return of Debit Entries) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Determine through review of procedures and inquiry with management, that the Written Statements of Unauthorized Debit are provided to the ODFI within 10 banking days from the receipt of the written request of the ODFI.</p>	<p>All return entries must be returned to the ACH Operator in accordance with Appendix Four – Return Entries, on page OR 139 of NACHA rule book</p> <p>A permissible return entry is return code R31. The Financial Institution you are auditing should only accept this return if they have provided prior notice (verbally or in writing) that they would be willing to accept the return.</p> <p>The Financial Institution can either accept a dishonored return, correct a dishonored return, or contest a dishonored return. Corrections and contested returns must be sent to the ACH Operator within two banking days after the settlement date of the dishonored return entry.</p> <p>NACHA Rule Book</p> <ul style="list-style-type: none"> - RDFI’s Right to Transmit Return Entries, OR 47 - Late Return Entries for CCD or CTX Entries with ODFI Agreement, OR 48 - Receipt of Dishonored Returns, OR 48 - Appendix Four – Return Entries, OR 139 <p>Subsection 3.8.3.5 Late Return Entries for CCD or CTX Entries with ODFI Agreement</p> <p>Subsection 3.8.5 Receipt of Dishonored Returns</p>

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (RDFI Timely Return of Debit Entries) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Document the process for returning ARC, BOC, POP and TEL entries and the reason code used by the financial institution to return these.</p> <p>Review transmittal reports for returns and archives and select a sample of entries returned with codes R05, R07, R10, R37, R51, & R53. Verify that each return is supported by a signed "Written Statement of Unauthorized Debit". If no entries are observed, obtain the statements from the ACH Operator for the audit period and determine that there were no "Unauthorized Entry Fees" being received during this time period.</p> <p>For each transaction, obtain documentation to support that the transaction being returned is accurately represented within the WSUD, the WSUD was signed by the account holder, the appropriate return reason code was utilized, and the return was process in accordance with the timelines set forth by NACHA.</p> <p>Through review of posting journals determine whether the financial institution receives "wholesale credit" ACH Activity subject to UCC 4A (credits with Standard Entry Codes CCD and CTX). The notices should include the following:</p> <ol style="list-style-type: none"> a) the Entry may be Transmitted through the ACH; b) the rights and obligations of the Receiver concerning the Entry are governed by and construed in accordance with the laws of the State of New York, unless the Receiver and the RDFI have agreed that the laws of another jurisdiction govern their rights and obligations; c) credit given by the RDFI to the Receiver for the Entry as provided by Subsection 3.3.1 (Availability of Credit Entries to Receivers) is provisional until the RDFI has received final settlement through a Federal Reserve Bank or otherwise has received payment as provided for in Section 4A-403(a) of Article 4A; d) if the RDFI does not receive such payment for the Entry, the RDFI is entitled to a refund from the Receiver in the amount of the credit to the Receiver's account, and the Originator will not be considered to have paid the amount of the credit Entry to the Receiver; and e) these Rules do not require the RDFI to provide the Receiver with notice that the RDFI has received the Entry unless the RDFI has agreed to do so.

NACHA – Receiving Depository Financial Institution (RDFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (RDFI Timely Return of Debit Entries) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Through inquiry and observation, determine whether the following items have been disclosed to those accounts receiving such items:</p> <p>(Provisional Payment Disclosure) "Credit given by [us] to [you] with respect to an automated clearing house credit entry is provisional until [we] receive final settlement for such entry through a Federal Reserve Financial Institution. If [we] do not receive such final settlement, [you] are hereby notified and agree that [we] are entitled to a refund of the amount credited to [you] in connection with such entry, and the party making payments to [you] via such entry (i.e., the originator of the entry) shall not be deemed to have paid [you] in the amount of such entry."</p> <p>(Notice Disclosure) "Under the operating rules of the National Automated Clearing House Association, which are applicable to ACH Transactions involving your account, [we] are not required to give next day notice to [you] of receipt of an ACH item and [we] will not do so. However, [we] will continue to notify you of the receipt of payments in the periodic statements we provide to you."</p> <p>(Choice of Law Disclosure) "[We] may accept on [your] behalf payments to [your] account which have been transmitted through one or more Automated Clearing Houses (ACH) and which are not subject to the Electronic Fund Transfer Act and [your] rights and obligations with respect to such payments shall be construed in accordance with and governed by the laws of the state of [New York] as provided by the operating rules of the National Automated Clearing House Association, which are applicable to ACH transactions involving your account."</p> <p>Through inquiry, determine whether the financial institution can identify transactions containing payment-related information received with corporate entries with Standard Entry Class Codes CCD, CIE, CTX and IAT (addenda records). Determine the manner in which receivers may request the information that is included within the addenda records and the timing by which management complies with the request.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (ODFI Binding Agreements) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through review of the standard originator agreement, determine the agreement addresses the following issues:</p> <ul style="list-style-type: none"> a) The Originator must authorize the ODFI to originate Entries on behalf of the Originator to Receivers' accounts; b) The Originator must agree to be bound by these Rules; c) The Originator must agree not to originate Entries that violate the laws of the United States; d) Any restrictions on the types of Entries that may be originated; e) The right of the ODFI to terminate or suspend the agreement for breach of these Rules in a manner that permits the ODFI to comply with these Rules; and, f) The right of the ODFI to audit the Originator's compliance with the Origination Agreement and these Rules. g) For IAT entries, the agreement must specify (1) the terms and conditions for allocation of gains, losses and the assumption of risk for foreign exchange conversion, and (2) the rights and responsibilities of the ODFI in the event of an Erroneous Entry. 	<p>There is an extra requirement per NACHA for Third Party Sender agreements. That requirement is "The Third Party Sender must agree that, before permitting an Originator to originate any Entry directly or indirectly through the ODFI, it will enter into an agreement with the Originator that satisfies each of the requirements of Subsection 2.2.2.1 (ODFI Must Enter Origination Agreement with Originator). Many Financial Institutions use the same Originator agreement for their Third Party Senders and therefore the Third Party Sender agreement is thus silent on this requirement - See common audit findings.</p> <p>A NACHA rule change now requires Financial Institutions to register Third Party Senders with NACHA by March 1, 2018. Many Financial Institutions are going back and reviewing their Originators to determine if they are actually a Third Party Sender that needs to be registered with NACHA. You may want to see if the Financial Institution has identified any Originators that are actually Third Party Senders. If they have identified some, did the Financial Institution overlook the need to have an Originator execute a new agreement that meets the NACHA requirements for a Third Party Sender? If so this would be a finding - See common audit findings.</p> <p>NACHA Rule Book</p> <p>Section 2.2.2.1 - ODFI Must Enter Origination Agreement with Originator, page OR 5</p> <p>Section 2.2.2.2 -ODFI Must Enter Origination Agreement with Third-Party Sender, page OR 5</p> <p>Section 2.5.8.3 - Origination Agreements for IAT Entries, page OR 15</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Binding Agreements) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Section IV - Special Topics in the Operations Guidelines section of the Operating Rules Book for guidance on third party senders.) The ODFI should have an origination agreement with each third party for which the ODFI will initiate entries. The Origination Agreement must include the following:</p> <ul style="list-style-type: none"> a) The Third-Party Sender, on behalf of the Originator, must authorize the ODFI to originate Entries on behalf of the Originator to Receivers' accounts; b) The Third-Party Sender must agree to be bound by these rules; c) The Third-Party Sender must agree not to originate Entries that violate the laws of the United States; d) Any restrictions on the types of Entries that may be originated; e) The right of the ODFI to terminate or suspend the agreement, or any Originator of the Third-Party Sender, for breach of these Rules in a manner that permits the ODFI to comply with these Rules; f) The right of the ODFI to audit the Third-Party Sender's and its Originators' compliance with the Origination Agreement and these Rules; and g) The Third-Party Sender must agree that, before permitting an Originator to originate any Entry directly or indirectly through the ODFI, it will enter into an agreement with the Originator that satisfies each of the requirements of Subsection 2.2.2.1 (ODFI Must Enter Origination Agreement with Originator). <p>Determine whether the financial institution originates ACH files to the ACH Operator through a correspondent financial institution or third-party processor (sending point). (See Section IV - Special Topics in the Operations Guidelines section of the Operating Rules Book for guidance on third party senders.) If so, review to ensure there is an agreement executed between the ODFI and the Sending Point for ACH origination, which legally binds parties to comply with ACH Rules and establishes security procedures.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (ODFI Sending Point Agreements) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Through review of policies and procedures, determine whether the financial institution has a process to assess nature of originator’s activity and the risk it presents. Determine that the ODFI performs due diligence that, at a minimum includes:</p> <ul style="list-style-type: none"> a) assess the nature of the Originator’s or Third-Party Sender’s ACH activity and the risks it presents; b) establish, implement, and periodically review an exposure limit for the Originator or Third-Party Sender; and c) establish and implement procedures to: <ul style="list-style-type: none"> i. monitor the Originator’s or Third-Party Sender’s origination and return activity across multiple Settlement Dates; ii. enforce restrictions on the types of Entries that may be originated; and iii. enforce the exposure limit. d) has processes in place to terminate, suspend, or audit any originator or third-party sender if the rules are breached, the originator causes the ODFI to breach the rules. 	<p>NACHA Rule Book ODFI Agreement with Sending Points, OR 6;</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description	Detailed Guidance
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Determine that the financial institution has established exposure limits for each ACH Originator and that the limits consider net settlement position where multiple applications are being processed (debit and/or credits). Document the process.</p>	<p>NACHA Rule Book ODFI Risk Management, OR 6</p> <p>Some systems allow Originators to submit a \$10k ACH file on Monday to be processed on Friday and submit another \$10k file on Tuesday that will be processed on Friday also. If the Originator has a daily exposure limit of \$10k then the system should reject one of the files that is to be processed on Friday. If the system allows the Originator to process \$20k on Friday when their daily limit is \$10k because they submitted files on different days - that's a problem. That's what it means to monitor exposure limits across multiple settlement dates.</p> <p>Subsection 2.2.3 ODFI Risk Management</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Document the procedures in place to review the determined exposure limits for necessary adjustments and document the individuals (department) responsible for approving any exposure limit adjustments. This should be performed on a periodic basis (usually annually).</p>
	<p>Determine if procedures and/or system capabilities have been implemented to monitor exposure limit access across multiple settlement dates. Additionally, determine the method in which the ODFI enforces restrictions on the types of Entries that may be originated.</p>
(Continued)	<p>Review and document the procedures used to monitor compliance with exposure limits and the manner the exceptions are reported and to whom.</p>
	<p>Verify that the population report meets all request requirements and that the report is complete by performing one of the following procedures:</p> <ul style="list-style-type: none"> - reconcile the population report to an independent, reliable source - review the report query to verify that the report is designed to pull data from all transaction types and the time period requested. <p>Document population report verification results in the Population Complete text field under the Sampling Details section of the procedure. Attach any relevant supporting documentation to the procedure.</p>
	<p>Select samples from the population report based on the sampling methodology. Save the sample selection in a separate document and revise the sampling request item description to align to the needs of the remaining test steps. Work with your team members to communicate the sampling requests to the Client Service Manager or other appropriate client contact.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Select a sample of originators and determine the following: The standard origination agreement was executed with the originator.</p> <ul style="list-style-type: none"> a) The agreement was executed by both the Institution and the client. An agreement is on file and indicates type of entries to be originated; b) Assessment of Originator activity and risk it presents (example- risk assessment) c) Exposure limit and entry type restrictions have been established and authorized in accordance with policy; and d) Annual/Periodic review has been performed.
<p>(Continued)</p>	<p>Determine that the ODFI accepts all types of returns that comply with Appendix Four. Determine the manner in which return fees are initiated and how management confirms compliance with Subsection 2.14 - Return Fee Entries.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Determine that the Originator can identify that a return should be returned as dishonored, that the ODFI returns the items as dishonored within five banking days after the Settlement Date of the original return. Determine how the ODFI determine eligibility of a return to be dishonored:</p> <p>Eligibility:</p> <p>An ODFI may dishonor a Return Entry, with the exception of an IAT Return Entry, if:</p> <ul style="list-style-type: none"> a) the RDFI failed to return the Entry within the time limits established by these Rules; b) information in one or more of the following fields of the Return Entry is incorrect or missing: (i) DFI Account Number; (ii) Original Entry Trace Number; (iii) Amount; (iv) Individual Identification Number/Identification Number; (v) Transaction Code; (vi) Company Identification Number; (vii) Effective Entry Date; c) the Return Entry was misrouted; d) the Return Entry was a duplicate; e) the Return Entry is coded as the Return of an Erroneous Entry at the request of the ODFI, as permitted by Subsection 2.12.2 (ODFI Request for Return), but the ODFI did not make such a request; f) the Return Entry is coded as a permissible Return Entry, as permitted by Subsection 3.8.3.5 (Late Return Entries for CCD or CTX Entries with ODFI Agreement), but the ODFI did not agree to accept the Return Entry; g) the Return Entry would result in an unintended credit to the Receiver because <ul style="list-style-type: none"> i. the Return Entry relates to a debit Erroneous Entry, (2) the ODFI has already originated a credit Reversing Entry to correct the Erroneous Entry, and (3) the ODFI has not received a Return of that credit Reversing Entry; or h) the Return Entry would result in an unintended credit to the Receiver because <ul style="list-style-type: none"> i. the Return Entry relates to a debit Reversing Entry that was intended to correct a credit Erroneous Entry, and (2) the ODFI has not received a Return of that credit Erroneous Entry.

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p>	<p>Determine if the ODFI accepts contested dishonored returns.</p>
	<p>Document the procedure for handling NOCs and Corrected NOCs when received from RDFIs. Document how the information is relayed to the Originator of the transaction and the time frame (should be provided within two banking days of receipt) and the information as required by NACHA Rules is included in the communication with the originator. Consider selecting an example of a returned NOC received by the ODFI that was communicated to the Originator and test for compliance with items (a) – (n) in Subsection 2.11.1 ODFI and Originator Action on Notification of Change (NOC) of NACHA’s Rule Book.</p>
	<p>Document the process in place to ensure that Originators have made the requested changes based on the following conditions:</p> <ol style="list-style-type: none"> 1) NOCs related to prenotification entries - the opening of business on the 2nd banking day following the settlement date of the prenotification entire; 2) All other NOCs - within six banking days or prior to initiating the next entry, whichever is later.
	<p>Determine that refused Notices of Change are sent back to the RDFI within 15 days of receipt of the Notice of Change or Corrected Notice of Change. (OG54 – OG55)</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Discuss with management the ODFI's procedures when a request is received from an RDFI requesting a copy of the ACH entry authorization signed by the receiver.</p>
	<p>Determine if any such requests have been received from RDFIs by the ODFI since the last NACHA Self Audit and test to determine that the copy of the authorization was sent at no cost to the RDFI within 10 banking days of the receipt of the written request from the RDFI.</p>
	<p>Determine the procedure for handling RDFI requests for late returns for entries. (ODFI may agree, verbally or in writing, to accept the late return entry. The entry must be in the amount of the debit entry and be handled like all other returns.)</p>
	<p>Document the method used to identify initiating entries subject to UCC4A (Companies sending credit entries under Standard Entry Codes CCD or CTX). (UCC 4A applies only to corporate to corporate ACH credit transfers. It does not apply to any debit transfers or credit transfers covered by Regulation E. - That is, almost all credit transfers involving a consumer.)</p>
	<p>Discuss with management the procedures in place to comply with UCC4A with respect to corporate entries.</p>
<p>Through review of the company agreements for such Originators, observe whether the agreements identify the type of entries being originated and that they are subject to UCC4A.</p>	

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Through inquiry of Financial Institution personnel and review of disclosures, determine whether the following UCC4A disclosures have been distributed to companies initiating credit entries subject to UCC4A</p> <p>[Security Disclosure] [Company] and [financial institution] shall comply with the security procedure requirements described in the attached schedule/exhibit attached hereto with respect to entries transmitted by [company] to [financial institution].</p> <p>[Provisional Payment Disclosure] Credit given by the Receiving Depository Financial Institution (RDFI) to the Receiver with respect to credit entries subject to Uniform Commercial Code Appendix 4A (UCC4A), is provisional until the RDFI has received final settlement through a Federal Reserve Financial Institution or otherwise has received payment as provided in Section 4A-403(a) of UCC4A, and if such settlement or payment is not received, the RDFI shall be entitled to a refund of the amount credited from the Receiver, and the Originator shall not be deemed to have paid the Receiver the amount of the entry.</p> <p>[Choice of Law Disclosure] This agreement shall be construed in accordance with and governed by the laws of the state of [New York].</p> <p>Determine the method that management uses to establish the identity of each Originator or Third-Party Sender that uses an Unsecured Electronic Network.</p> <p>If there is a Third Party sender, document the process in which management has determined that the Third Party Sender has establish the identity of each Originator.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Discuss with Management the ODFI’s procedures for transmitting a reversing file and a reversing entry. Determine how management confirm eligibility of the reversing file/entry.</p> <p>An Originator or the ODFI must Transmit each Reversing File and, when appropriate, a corresponding Correcting File, to the ACH Operator within five Banking Days after the Settlement Date of the Erroneous File. The Originator or ODFI must Transmit the Reversing File and any corresponding Correcting File to the ACH Operator within twenty-four hours of the discovery of the Erroneous File. Any debit Entry within the Reversing File must not contain an Effective Entry Date that is earlier than the Effective Entry Date of the credit Entry to which it relates.</p> <p>An Originator may initiate a Reversing Entry to correct an Erroneous Entry previously initiated to a Receiver’s account. The Reversing Entry must be Transmitted to the ACH Operator in such time as to be Transmitted or made available to the RDFI within five Banking Days following the Settlement Date of the Erroneous Entry.</p> <p>A debit Reversing Entry must not contain an Effective Entry Date that is earlier than the Effective Entry Date of the credit Entry to which it relates.</p> <p>Inquire of management if reversing files have been transmitted to RDFIs since the prior NACHA Self Audit. Review the documentation for the reversing files to determine that they were transmitted on a timely basis.</p> <p>If the ODFI has transmitted reversing entries since the last NACHA Self Audit, determine that the entry(ies) had been processed on a timely basis.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Determine the method that management uses to establish the identity of each Originator or Third-Party Sender for BOC.</p>
	<p>If there is a Third Party sender, document the process in which management has determined that the Third Party Sender has established the identity of each Originator.</p>
	<p>Prior to originating BOC entries the ODFI has established procedures to document the following related to the originator of each BOC transaction:</p> <ul style="list-style-type: none"> a) company b) address c) telephone number d) contact person e) taxpayer identification number f) description of the nature and business of each Originator
	<p>Determine the established procedures for ensuring that the above noted information is sent to the RDFI upon request within two banking days of the receipt of the RDFI’s written request, provided the request is received within two years of the settlement date of the BOC entry.</p>
	<p>Discuss with Management the ODFI’s procedure for complying with the National Association’s request for information with respect to the ODFI’s Originators or Third-Party Senders. Determine that the ODFI’s procedures are in compliance with Article Two, Subsection. 2.17.2.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Inquire as to whether or not the ODFI has received such a request from the National Association. If so, review the documentation submitted to the National Association to determine that all information as required by Article Two, Subsection 2.18 was included in the transmission. Also, determine that the information was transmitted to the National Association within 10 banking days of receipt of the request.</p> <p>Inquire of Management whether or not the ODFI has entered in a Direct Access relationship with one or more third parties.</p> <p>a) If the ODFI does have one or more Direct Access Debit Participant relationships, the ODFI, the ODFI must register each relationship with the National Association. See Article Two, Subsection 2.19 for the information which must be included in the registration to the National Association. Obtain evidence that the ODFI's Board of Directors, or its designee has approved the Direct Access Debit Participant relationship.</p> <p>b) If the ODFI does not have any Direct Access Debit Participant relationships, the ODFI must provide the National Association with the following information:</p> <ul style="list-style-type: none"> i. The ODFI's routing number ii. The name, title, telephone number and address for a contact person at the ODFI, and iii. A statement acknowledging that the ODFI has no Direct Access Debit Participants.

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Inquire of Management whether or not the ODFI originates entries for any Third-Party Senders.</p> <ul style="list-style-type: none"> a) If the ODFI does originate entries for one or more Third Party Sender, the ODFI, the ODFI must register each relationship with the National Association. See Article Two, Subsection 2.17.3.1 for the information which must be included in the registration to the National Association. b) If the ODFI does not originate entries for any Third-Party Sender, the ODFI must provide the National Association with the following information: <ul style="list-style-type: none"> i. The ODFI’s routing number ii. The name, title, telephone number and address for a contact person at the ODFI, and iii. A statement acknowledging that the ODFI has no Third Party Senders.
	<p>Document the method the ODFI uses to ensure Originators are continually kept informed of their obligations with respect to these rules.</p>
	<p>Through discussion with management and review of policies and procedures, determine the manner in which WEB entries to consumer accounts are initiated, authorization by the consumer is authenticated, and information related to the transaction, including account and routing numbers, are validated. Determine what fraud detection systems are in place and the frequency with which the systems are validated.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Select a sample of Originators who originate TEL and WEB debit entries, obtain documentation that the ODFI has confirmed that each originator has:</p> <p>Fraud Detection Systems. The Originator has established and implemented a commercially reasonable fraudulent transaction detection system to screen the debit WEB Entry.</p> <ul style="list-style-type: none"> a) Verification of Receiver’s Identity. The Originator has established and implemented commercially reasonable methods of authentication to verify the identity of the Receiver of the debit WEB Entry. b) Verification of Routing Numbers. The Originator has established and implemented commercially reasonable procedures to verify that the routing number used in the debit WEB Entry is valid. c) Contractual Elements - Determine that the above items are included within the ACH agreement between the ODFI and the originator. <p>Select a sample of Originators who originate WEB debit entries, obtain evidence that the originator, within the last 12 months, conducted or had conducted on its behalf, and annual audit to ensure that the financial information it obtains from Receivers is protected by security practices and procedures that include, at a minimum, adequate levels of:</p> <ul style="list-style-type: none"> a) physical security to protect against theft, tampering, or damage; b) personnel and access controls to protect against unauthorized access and use; and c) network security to ensure secure capture, storage, and distribution.

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Select a sample of CIE and WEB credit entries originated by the Bank. Obtain the monthly account statement from the applicable deposit account and confirm the following information is included with respect to each WEB credit entry:</p> <ul style="list-style-type: none"> a) the date funds were debited from the Consumer’s Account for the purpose of funding the credit WEB Entry; b) dollar amount of the funds debited; c) payee name; d) a description of the payment; e) account type; f) account number; g) amount of any charges assessed against the account for services related to the Entry; h) balances in the Originator’s account at the beginning and at the close of the statement period; and i) address and telephone number to be used for inquiries or notices of errors preceded by “Direct Inquiries To” or similar language. <p>© 2019 NACHA — The Electronic Payments Association®</p> <p>Content copied from https://www.nachaoperatingrulesonline.org/2.15497/s012/ss076-1.4276515</p> <p>Through discussion with management and review of policies and procedures, determine the manner in which RCK (re-presented check entry) entries are originated and how management determines the item eligibility for being transmitted as an RCK entry.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Select a sample of originated RCK entries, determine the eligibility/ineligibility of the by as follows:</p> <p>Eligible Items - An Originator may initiate an RCK Entry only in relation to an item that:</p> <ul style="list-style-type: none"> a) (a) is an item within the meaning of Revised Article 4 of the Uniform Commercial Code (1990 Official Text); b) (b) is a negotiable demand draft drawn on or payable through or at a Participating DFI, other than a Federal Reserve Bank or Federal Home Loan Bank; c) (c) contains a pre-printed serial number; d) (d) is in an amount less than \$2,500; e) (e) indicates on the face of the document that the item was returned due to “Not Sufficient Funds,” “NSF,” “Uncollected Funds,” or comparable language; f) (f) is dated 180 days or less from the date the RCK Entry is Transmitted to the RDFI (i.e., the item to which the RCK Entry relates is not stale-dated); g) (g) is drawn on a Consumer Account; and h) (h) has been previously presented: <ul style="list-style-type: none"> i. no more than two times through the check collection system (as a Check, substitute check, or image), if the Entry is an initial RCK Entry; or ii. no more than one time through the check collection system (as a Check, substitute check, or image), and no more than one time as an RCK Entry, if the Entry is a reinitiated RCK Entry in accordance with Subsection 2.12.4.1 (General Rule for Reinitiated Entries). <p>Ineligible Items:</p> <ul style="list-style-type: none"> a) noncash items (as defined in Section 229.2(u) of Regulation CC); b) drafts drawn on the Treasury of the United States, a Federal Reserve Bank, or a Federal Home Loan Bank; c) drafts drawn on a state or local government that are not payable through or at a Participating DFI; d) United States Postal Service money orders; e) items payable in a medium other than United States currency; f) items payable to a person other than the Originator; and (g) drafts that do not contain the original signature of the Receiver, including remotely created checks, as defined by Regulation CC. <p>© 2019 NACHA — The Electronic Payments Association®</p> <p>Content copied from https://www.nachaoperatingrulesonline.org/2.15497/s012/ss072-1.4276490</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Through discussion with management and review of policies and procedures, determine how the ODFI conveys the authorization requirements related to TEL entries to the Originator. Determine how the ODFI confirms that authorization is recorded, or a written confirmation of oral authorization was provided prior to the settlement date of the TEL entry. Determine how management has confirmed that the Originator is obtaining the minimum required information as outlined by NACHA.</p> <p>Through discussion with management and review of policies and procedures, determine the manner in which XCK (destroyed check entries) will be initiated and how management determines the eligibility of the items.</p> <p>Select a sample of originated XCK entries, determine the eligibility/ineligibility of the by as follows:</p> <p>Eligible Items:</p> <ul style="list-style-type: none"> a) is an item within the meaning of Article 4 of the Uniform Commercial Code; b) is a negotiable demand draft drawn on or payable through or at an office of a Participating DFI, other than a Federal Reserve Bank or Federal Home Loan Bank; c) is in an amount less than \$2,500; and d) either : <ul style="list-style-type: none"> (1) is contained in a cash letter that is lost, destroyed, or otherwise unavailable while in transit for presentment to a paying bank, and cannot be obtained; or (2) (i) is missing part of the MICR line but can be sufficiently repaired to create an ACH Entry; (ii) is an image of an item that cannot be processed through the applicable image exchange, but has sufficient information to create an Entry; or (iii) is, in whole or in part, unreadable, obscured, or mutilated in a manner that prevents automated check processing or creation of an image that can be used to produce a “substitute check” that is the legal equivalent of the original check under the Check Clearing for the 21st Century Act, Pub. L. 108-100, but has sufficient information to create an Entry. <p>Ineligible Items</p> <ul style="list-style-type: none"> a) noncash items (as defined in Section 229.2(u) of Regulation CC); b) drafts drawn on the Treasury of the United States, a Federal Reserve Bank, or a Federal Home Loan Bank; (c) drafts drawn on a state or local government that are not payable through or at a Participating DFI; d) United States Postal Service money orders; e) items payable in a medium other than United States currency; and (f) returned items.

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Through discussion with management and review of policies and procedures, determine the process surrounding the sending of prenotification entries and originating subsequent entries to the receiver's account to which the prenotification relates. Determine that subsequent entries are not transmitted any sooner than three banking days following the settlement date of the prenotification entry, provided the ODFI has not received a Return or a Notification of Change related to the Prenotification. Determine if the control in place is system driven. If system driven, obtain evidence supporting the system control not permitting the subsequent transactions earlier than three business days after the settlement date of the prenotification entry.</p> <p>Select a sample of prenotification entries, obtain documentation supporting that there were no subsequent transactions originated within three banking days of the settlement date of the prenotification entry.</p>

NACHA – Originating Depository Financial Institution (ODFI)

Risk Statement	Test Step Description
<p>Non-compliance with NACHA Rules (ODFI Exposure Limits) can lead to fines as outlined in NACHA rule book - Appendix 10. Fines can be up to \$500,000 per month until violation is resolved. Additionally, the Financial Institution could face suspension of ACH processing rights if rule violations are not resolved.</p> <p>(Continued)</p>	<p>Through discussion with management and review of policies and procedures, determine the manner in which reclamation entries and written demand for payment entries are initiated and how management determines eligibility and amount of the items:</p> <p>An Originator or ODFI may initiate a Reclamation Entry or written demand for payment with respect to a previously Transmitted credit Entry to a Receiver’s account under the following circumstances: (</p> <p>a) The Receiver has died and the Receiver’s right to receive one or more pension, annuity, or other benefit payments has terminated before the receipt by the RDFI of one or more credit Entries to the Receiver’s account; and</p> <p>(b) Neither the Receiver’s estate nor any other holder of the account is entitled to the payments.</p> <p>An Originator or ODFI must not initiate a Reclamation Entry or written demand for payment in an amount that exceeds the amount of any payment to which the Receiver was not entitled.</p> <p>An Originator or ODFI must originate a Reclamation Entry or written demand for payment within five Banking Days after the Originator receives notice of the death of the Receiver. If a Reclamation Entry is returned by the RDFI, the Originator may make a written demand for payment within fifteen Banking Days after it receives the returned Reclamation Entry. For this subsection, notice received by the Originator is considered to be effective from the time specified in Section 1-202(f) of the Uniform Commercial Code.</p> <p>A Reclamation Entry must not contain an Effective Entry Date that is earlier than the Effective Entry Date of the credit Entry to which it relates.</p> <p>Select a sample of reclamation entries and written demand for payment entries. Obtain evidence that the entries met the eligibility requirements, was in the proper amount, and was transmitted within the timelines outlined in Subsection 2.10 of the NACHA Rules</p>



NACHA Rules Updates

Cost of NACHA Non-Compliance

- NACHA Rules - Appendix Ten Rules Enforcement
- Fines and Penalties Separated into 3 Classes
 - Class 1
 - Class 2
 - Class 3
- First Occurrence: \$1,000
- Last Occurrence: \$500,000 and suspension from ACH Processing

Same Day ACH



- In a nutshell, payments will settle in the same day
- United States has one of largest payment systems but not the fastest
- Result of E-commerce and customer demand for better cash flow

Same Day ACH

Same –Day ACH Payments: Phased Approach

FUNCTIONALITY	PHASE 1: SEPT. 23, 2016	PHASE 2: SEPT. 15, 2017	PHASE 3 MAR. 16, 2018
Transaction eligibility (\$25,000 limit) (international transactions not eligible)	Credits only	Credit and debits	Credit and debits
New ODFI ACH file transmission times	10:30 a.m. ET 2:45 p.m. ET	10:30 a.m. ET 2:45 p.m. ET	10:30 a.m. ET 2:45 p.m. ET
New settlement times	1 p.m. ET 5 p.m. ET	1 p.m. ET 5 p.m. ET	1 p.m. ET 5 p.m. ET
ACH credit funds availability	End of RDFI's processing day ¹	End of RDFI's processing day ¹	5 p.m. RDFI's local time ²

Source: Reserve Bank of Dallas presentation at Texpo 2016, Crowe analysis

Next Steps for Same Day ACH

Increases the per-transaction dollar limit for Same Day ACH transactions to \$100,000

- Currently, Same Day ACH transactions are limited to \$25,000 per transaction
- While the current limit covers approximately 98% of ACH transactions, there are many use cases for which a higher dollar limit will better enable end users to utilize Same Day ACH. For example, a higher transaction limit would better enable:
 - B2B payments, in which only approximately 89% of transactions are currently eligible
 - Claim payments, which are often for larger dollar amounts and are time sensitive in nature
 - Reversals for a larger pool of transactions, including all Same Day ACH transactions

Target Implementation: March 20, 2020

Source: NACHA

Next Steps for Same Day ACH

Creates a third Same Day ACH processing window that expands Same Day ACH availability by 2 hours

- Currently, the latest that an ODFI can submit files of Same Day ACH transactions to an ACH Operator is 2:45 p.m. ET (11:45 a.m. PT)
- The new window will allow Same Day ACH files to be submitted until 4:45 p.m. ET (1:45 p.m. PT), providing greater access for all ODFIs and their customers
- The timing of this new processing window is intended to balance the desire to expand access to Same Day ACH through extended hours with the need to minimize impacts on financial institutions' end-of-day operations and the re-opening of the next banking day

Target Implementation: September 18, 2020

Source: NACHA

Third-Party Sender (TPS) vs. Third-Party Provider

ACH Third-Party Service Providers (TPSP)

- Originates ACH on behalf of **an FI's** customer
- ACH Origination agreement is with **the FI** customer
- ACH settlement account: **the FI customer's account**
- Separate stand-alone agreement between FI and the (TPSP) recommended

ACH Third-Party Senders (TPS)

- Originates ACH on behalf of **their** customers
- ACH agreement **with TPS, not** their customer
- ACH settlement account: **TPS' account**



Polling Question #3

Following this session, do you have a better understanding of how conduct an audit over electronic funds transfer?

- A. Yes
- B. Somewhat
- C. Not really



Auditing the Deposit Function

Presented by Stacia Schacter



Polling Question #1

How comfortable are you when it comes to conducting audits over the deposit function?

- A. Very comfortable
- B. Fairly comfortable
- C. Only slightly comfortable
- D. What are deposits?

Procedures Assessment

Essential Control Point

Written procedures exist and describe the critical processes and controls within this activity.

Program Steps

Assess the following for the procedures related to this activity:

1. Existence:

Do procedures exist for this activity?

If not, should the institution have them?

2. Current:

Are procedures a reflection of current practice and controls?

3. Completeness:

Are procedures complete with respect to critical elements of the activity and the critical control points?

Opening and Closing Accounts

Essential Control Points

- New accounts are reviewed for input accuracy and required documentation.
- New accounts are opened by authorized individuals.
- Missing documentation on deposit accounts is monitored for timely resolution.

Program Steps

- Discuss with management the process for reviewing new accounts input and documentation. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Select a sample of new deposit accounts (include all types of accounts in the sample) and test for the following attributes:
 1. A completed signature card is on file.
 2. Customer's identity was confirmed and documented as required by the policy.
 3. The customer's TIN# was verified against ChexSystems or similar reporting agency.
 4. The W-9 Tax Payor ID certification or W-8 Foreign Status certification portion of the account documentation is complete and signed by the customer.
 5. The customer's name and address are accurately recorded on the system.
 6. The account type as stated on the signature card is equivalent to the system set up.

Polling Question #2

Which of the following are essential control points for opening and closing accounts?

- A. New accounts are reviewed for input accuracy and required documentation.
- B. New accounts are opened by authorized individuals.
- C. Missing documentation on deposit accounts is monitored for timely resolution.
- D. All the above.



Opening and Closing Accounts

Essential Control Points

- New accounts are reviewed for input accuracy and required documentation.
- New accounts are opened by authorized individuals.

Program Steps

Obtain a report from management of deposit accounts with Post Office (PO) Boxes.

Request that the report be sorted by PO Box.

Review the report to identify multiple accounts with the same PO Box.

Select a sample that appear to be unrelated and obtain documentation to support the validity of the account.



Opening and Closing Accounts

Essential Control Point

Missing documentation on deposit accounts is monitored for timely resolution.

Program Steps

- Obtain a report of accounts with blank names or no TINs. Determine if the accounts are included on the report of missing documentation. Discuss with management the procedures performed to resolve the issues.
- Obtain the most recent report of missing documentation on deposit accounts. Review the report for items that are over 30 days outstanding. Discuss with management the procedures for resolving the items.



Opening and Closing Accounts

Essential Control Point

New accounts are monitored for unusual and/or uncollected fund activity.

Program Steps

Discuss with management the process for monitoring new accounts for unusual and uncollected fund activity. Document the process, considering the following:

1. Responsible individuals
2. Frequency of review
3. Procedures for follow-up as unusual activity is identified.

Opening and Closing Accounts

Essential Control Point

Written documentation to support account closings is maintained.

Program Steps

- Obtain a report of accounts flagged as "closed" with balances. Select a sample from the report, discuss each scenario with management. Determine and document the cause and resolution for each selected account.
- Select a sample of closed accounts and determine if the account was closed at the bank's request, customer's request or from maintaining a zero balance for a consecutive number of days. Test each scenario for the following attributes:
 - Accounts closed at the bank's request:
 1. Written authorization from the appropriate level of management was obtained to close the account.
 2. Trace any negative balances in the account to charge-off posting.
 - Accounts closed at customer request:
 1. Written authorization from the customer was obtained prior to closing. Trace the signature to the signature card.
 2. The account was closed within two business days of the request.
 - Accounts closed from maintaining a zero balance for a consecutive number of days:
 1. Obtain the transaction history of the account for the most recent three months having activity.
 2. Select a sample of withdrawals and/or checks paid and trace the signature to the signature card.

Opening and Closing Accounts

Essential Control Points

- Early withdrawal penalties for certificates of deposit are automatically assessed by the system in accordance with the terms of the signed agreement.
- Waived penalties are approved by authorized personnel and the approval is documented.

Program Steps

Select a sample of CD's closing prior to maturity. Test for the following attributes:

1. The account was assessed a penalty.
2. The penalty assessed was in accordance with the terms of the signed agreement.
3. The penalty recorded was calculated correctly.
4. If a penalty was not assessed, the waiver/refund was properly approved, and the approval documented.



Opening and Closing Accounts

Essential Control Point

Management monitors the number of closed accounts for significant increases in the reporting period.

Program Steps

Discuss with management the process to monitor trends on new and closed accounts for the total institution and region/branch. Document the process, considering the essential control points. Identify the level of monitoring performed by Senior Management and at the Board level. Obtain the reports presented to the Board of Directors and determine if the information presented is adequate for decision making.

Account File Maintenance

Essential Control Points

- File maintenance change reports are reviewed for unusual activity and reasonableness.
- File maintenance changes are compared to supporting documentation for input accuracy and authorization.
- File maintenance changes are made only by authorized/designated individuals.

Program Steps

- Discuss with management the file maintenance change process, from the point the request is made until the transaction has been posted. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and in operation. Select a transaction and walk it through the process as it touches each control point.
- Select a sample of file maintenance changes and review for supporting documentation and authorization.



Account File Maintenance

Essential Control Points

- File maintenance change reports are reviewed for unusual activity and reasonableness
- File maintenance changes are compared to supporting documentation for input accuracy and authorization

Program Steps

If file maintenance changes are reviewed by an individual with access to make changes, perform these additional procedures. Select a sample of file maintenance reports, and

1. Determine if evidence is present that the reports were reviewed by an individual other than the employee noted above.
2. Select a sample of file maintenance changes made by the individual noted above, and determine if evidence exists to support those changes were independently reviewed against supporting documentation.



Account File Maintenance

Essential Control Points

- File maintenance changes are compared to supporting documentation for input accuracy and authorization.
- File maintenance changes are made only by authorized/designated individuals.

Program Steps

If file maintenance changes are reviewed in separate departments, perform these additional procedures.

Select a sample of file maintenance reports, determine if a process is in place to identify file maintenance changes that have not been reviewed.



Account File Maintenance

Essential Control Point

- Written authorization for stop payment requests is obtained.

Program Steps

- Discuss with management the stop payment process, from the point the request is made until the request has been posted. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and in operation.
- Select a sample of stop payment transactions and determine if they were processed in accordance with the bank's procedures.

Overdraft & Uncollected Funds

Essential Control Points

- Overdrafts are decided on a daily basis by authorized individuals.
- Overdraft limits and fees have been established and approved by the Board of Directors.
- All overdraft decisions are independently reviewed for proper authorization.
- Drawings on uncollected funds and kiting suspect transactions are monitored for unusual activity. Overdrafts are charged off when deemed uncollectible or after a set number of days.
- The recovery of a previously charged off overdraft amount is recorded and reconciled in accordance with procedures and independent of the collections process.
- Overdrafts are monitored for compliance with charge off policy. Charge offs are approved by authorized individuals.

Program Steps

Discuss with management the process for monitoring and processing pay/return decisions on overdrafts. Discuss the process for charging off overdraw accounts. Discuss the processes for recording and reconciling the recovery of charged off overdrafts. Document the processes considering the essential control points. Comment on whether the controls are effectively designed and are in operation.



Overdraft & Uncollected Funds

Essential Control Points

- Overdrafts are decided on a daily basis by authorized individuals.
- Overdraft limits and fees have been established and approved by the Board of Directors.
- All overdraft decisions are independently reviewed for proper authorization.

Program Steps

Select a sample of overdrafts and test for the following attributes:

1. The decision to pay/return was made by an authorized individual.
2. The overdraft was within the limit of the approver.
3. Overdraft fees were charged to the account. If not, the waiver was approved.



Overdraft & Uncollected Funds

Essential Control Points

- Overdrafts are charged off when deemed uncollectible or after a set number of days.
- Overdrafts are monitored for compliance with charge off policy. Charge offs are approved by authorized individuals.

Program Steps

- Review the most recent overdraft report for items outstanding longer than allowed under policy/regulatory guidelines. Discuss the collection status with management.
- Select a sample of charged off overdrafts and determine that the charge-off was properly approved.
- Review the account to which overdraft charge-offs are posted and determine if the activity appears reasonable based on the current charge-off practice.



Overdraft & Uncollected Funds

Essential Control Points

Overdrafts are monitored for compliance with charge off policy. Charge offs are approved by authorized individuals.

Program Steps

Review the most recent overdraft report for items outstanding longer than allowed under policy/regulatory guidelines. Discuss the collection status with management.



Overdraft Protection

Essential Control Points

- Overall overdraft limits and fees have been established and approved by the Board of Directors.

Program Steps

- Discuss with Management the process of Overdraft Protection, from underwriting to approval of the Overdraft Protection relationship and the preparation and execution of the Overdraft Protection agreements. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Discuss with management the process for establishing and changing fees charged for Overdraft Protection privileges. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.



Overdraft Protection

Essential Control Point

- Completed and signed Overdraft Protection agreements are on hand for customers that have Overdraft Protection set up on the checking account with the institution.

Program Steps

- Select a sample of accounts with Overdraft Protection and determine if a completed and signed agreement is on hand.



Overdraft Protection

Essential Control Point

Fees are collected for overdrafts on accounts with Overdraft Protection in accordance with institution policy.

Program Steps

- Obtain a report of Overdraft Protection accounts set up to incur no service charges, discuss with management the nature of this type of waiver and the loss of potential income opportunities.
- Select a sample of Overdraft Protection accounts with fee waivers and review evidence to support the waiver was properly authorized.



Overdraft Protection

Essential Control Points

Overdraft accounts are monitored and charged off when deemed uncollectible or after a set number of days. Collection efforts are also performed on overdraft accounts charged off.

Program Steps

- Select a sample of charged-off overdrafts related to Overdraft Protection and determine that the charge-off was properly approved and charged off within the required timeframe.
- Review the account to which overdraft charge-offs on Overdraft Protection accounts are posted and determine if the activity appears reasonable based on the current charge-off practice. Discuss with management the process to record recoveries and methods to reconcile activity.



Overdraft Protection

Essential Control Point

Credit reviews are performed before accounts are approved for Overdraft Protection.

Program Steps

- Discuss with management the process performing credit reviews on accounts approved for Overdraft Protection. Comment on whether the controls are designed effectively and are in operation.



Overdraft Protection

Essential Control Points

Funds are automatically transferred on accounts with Overdraft Protection.

Program Steps

- Discuss with Management the process of sweeping funds to cover an overdraft for accounts with Overdraft Protection. Comment on whether the controls are designed effectively and are in operation.
- Select a sample of Overdraft Protection accounts and review evidence to support the sweeping of funds is automatic.

Dormant Accounts

Essential Control Points

- Dormant account periods are established for each type of account.
- Dormant accounts are escheated to the appropriate state in accordance within the specified time frames as required by state law.
- Management receives timely updates of changes to the escheatment laws regarding the handling and remitting of dormant account funds.
- Management periodically reviews the number and total dollar of the dormant account portfolio to identify trends in customer activity.
- Dormant accounts are automatically flagged by the system upon reaching the predetermined time frame of inactivity.
- Dormant account transactions are reviewed for written customer authorization.
- Written customer authorization is received prior accepting a transaction on a dormant account.
- Signature cards on dormant accounts are immediately restricted upon reaching the dormant status.
- Dormant accounts are reactivated only after receipt of written customer authorization or confirmation of the validity of the customer initiated monetary transaction.

Program Steps

Discuss with management the process for identifying, monitoring, and processing dormant accounts. Discuss the process for identifying and escheating dormant account funds to the state. Document the processes, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

Dormant Accounts

Essential Control Points

- Dormant account periods are established for each type of account.
- Dormant accounts are automatically flagged by the system upon reaching the predetermined time frame of inactivity.
- Dormant account transactions are reviewed for written customer authorization.
- Written customer authorization is received prior accepting a transaction on a dormant account.
- Signature cards on dormant accounts are immediately restricted upon reaching the dormant status.
- Dormant accounts are reactivated only after receipt of written customer authorization or confirmation of the validity of the customer initiated monetary transaction.

Program Steps

- Select a sample of reactivated dormant accounts. Identify the transaction initiating the reactivation. Trace the customer's signature to the signature card to determine that the transaction was properly authorized.
- For those accounts where customer authorization cannot be verified, obtain transaction history indicating all transactions performed since reactivation. Select an additional sample of withdrawals from each account and trace signature to the signature card. Discuss any exceptions identified with management.



Dormant Accounts

Essential Control Points

- Management periodically reviews the number and total dollar of the dormant account portfolio to identify trends in customer activity.

Program Steps

- Determine the frequency with which management reviews the dormant account portfolio. Determine if sufficient documentation is included to identify trends in customer activity.



Dormant Accounts

Essential Control Point

Dormant account transactions are reviewed for written customer authorization.

Program Steps

Obtain dormant activity reports for a sample of days. Determine if written evidence is present to support that the reports were reviewed by an individual independent of transaction capabilities.



Dormant Accounts

Essential Control Points

- Dormant accounts are escheated to the appropriate state in accordance within the specified time frames as required by state law.
- Management receives timely updates of changes to the escheatment laws regarding the handling and remitting of dormant account funds.

Program Steps

Obtain a report of all dormant accounts that includes the date of last activity and date of dormancy status. Review the list to determine if accounts are within the reporting timeframe.

Income & Expense Recognition

Essential Control Points

- Master file change reports are reviewed to identify unauthorized changes.
- Management has identified the individuals authorized to perform master-file changes.
- Master file changes are compared to supporting documentation for input accuracy and authorization.
- Management periodically analyzes the composition of the portfolio, deposit growth, deposit account related income and expense for the institution and on a cost center basis.
- Management has identified the individuals authorized for approving interest rates outside of the established rate parameters.

Program Steps

- Discuss with management the process for changing interest rates on deposit accounts, from the decision to change the rates through the input/review of the actual change on the system. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Select a sample of each type of deposit account, including all interest plans, and test for the following attributes:
 1. the interest rate is accurate and authorized.
 2. the system is accurately calculating the accrued interest based on the account disclosures.
- Obtain a report of high and low rate interest bearing accounts. Determine if rates are accurate and authorized.

Income & Expense Recognition

Essential Control Points

- Master file change reports are reviewed to identify unauthorized changes.
- Master file changes are compared to supporting documentation for input accuracy and authorization.
- Management periodically analyzes the composition of the portfolio, deposit growth, deposit account related income and expense for the institution and on a cost center basis.
- Fee waivers on deposit account are only done by authorized individuals
- Hard-code fee waivers and fee reversals are properly authorized and documentation is retained.

Program Steps

Discuss with management the process for establishing and changing fees on personal and commercial deposit accounts. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.



Income & Expense Recognition

Essential Control Point

Fee waivers on deposit account are only done by authorized individuals.

Program Steps

Obtain a report of deposit accounts set up to incur no service charges, discuss with management the nature of this type of waiver and the loss of potential income opportunities. Select a sample of deposit accounts set up to incur no service charge and review evidence to support the waiver was properly authorized.



Income & Expense Recognition

Essential Control Points

- Fee waivers on deposit account are only done by authorized individuals.
- Hard-code fee waivers and fee reversals are properly authorized and documentation is retained.

Program Steps

Select a sample of hard-code fee waivers and reversals on deposit accounts. Determine that the waiver or reversal was properly authorized in writing.



Income & Expense Recognition

Essential Control Point

Master file change reports are reviewed to identify unauthorized changes.

Program Steps

Select a sample of accounts that underwent an automatic rate change. Determine that the rate changed accurately. For tiered accounts, determine that the account met the balance requirements as stated in the agreement.



Income & Expense Recognition

Essential Control Point

Management periodically analyzes the composition of the portfolio, deposit growth, deposit account related income and expense for the institution and on a cost center basis.

Program Steps

Determine the frequency with which management reviews the performance of the deposit portfolio. Obtain management's most recent review and determine if sufficient documentation is included to allow for prudent evaluation and decision making for the overall institution as well as the individual branch/cost center.

Example of Check Fraud

A group of 18 defendants was charged with operating an identity theft ring that used information obtained from tellers at New York City banks to generate counterfeit checks from hundreds of accounts.

Prosecutors charged that the ring collected personal and bank account information belonging to 500 people by paying off bank tellers and also by buying copies of legitimate payroll checks. Thousands of counterfeit checks were manufactured with the information.

From a Bronx apartment known as “the Lab,” the leaders of the ring used specialized computer software, scanners, printers, check stock, magnetic ink, and company logos found on the Internet to produce the fake checks, which were cashed by “soldiers” enlisted for the scheme.

Example of Kite Fraud

BCSB Bankcorp Inc. of Baltimore announced that it would take an after-tax charge of **\$6.9 million**, because of losses from a check-kiting scheme. The charge, is likely to wipe out BCSB's earnings for this fiscal year.

Carrollton Bancorp in Baltimore will take a **\$1.2 million** after-tax charge to earnings after falling victim to a check-kiting scheme. The \$350 million-asset Carrollton is the second Baltimore banking company to be duped by the scheme.

The president and chief executive officer of BCSB resigned Monday, four weeks after the Baltimore company revealed that it lost millions in a check-kiting scheme allegedly carried out by one of its commercial customers.



Polling Question #3

Following this session, do you have a better understanding of how conduct an audit over the deposit function?

- A. Yes
- B. Somewhat
- C. Not really



Auditing the Branch Operations Function

Presented by Layne McGuire



Polling Question #1

How comfortable are you when it comes to conducting audits over the branch operations function?

- A. Very comfortable
- B. Fairly comfortable
- C. Only slightly comfortable
- D. What are branches?



Reconcilements

Essential Control Points

- General ledger or internal demand account reconciliations are reviewed in a timely manner for accuracy and completeness by an individual independent of its preparation.
- Reconciling items for general ledger and internal demand account reconciliations are cleared in a timely manner by an individual who is independent of the preparation of the reconciliations.
- General ledger accounts and internal demand accounts are reconciled in a timely manner to supporting detail by an individual who does not authorize or record transactions.

Reconcilements (Continued)

Audit Procedures

- Prepare a lead sheet of all general ledger and internal demand accounts utilized in the audit.
- Based on discussions with management, document the process for preparing and reviewing reconciliations, including auto-balance reconciliation, manual reconciliations, in-process and suspense accounts, internal DDAs, etc. Additionally, document the process of researching and clearing reconciling items. Consider the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Consider the following at a minimum:
 - Who prepares the reconciliation(s) and their other responsibilities within the institution and whether they conflict with the reconciliation process,
 - Frequency of the reconciliation(s),
 - Whether an independent review exists, **and**
 - The process for researching, resolving and/or elevating reconciling items to management.
- Document the process considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

Reconcilements (Continued)

Audit Procedures

- Using the lead sheet, select a sample of balance sheet (to include suspense, clearing, and zero-balance accounts) and internal DDA accounts to determine the following:
 - Sub-System and general ledger totals traced to support documentation.
 - The reconciliation was mathematically accurate.
 - The reconciliation was performed and in a timely manner,
 - The individual who prepared the reconciliation was independent of the authorization or recording functions, and
 - The reconciliation was subject to independent review and the review is documented.
- Review for stale dated reconciling items (i.e., 30 days for daily reconciliation, 90 days for a monthly reconciliation). Test selected items for legitimacy and proper clearing.

Cash

Essential Control Points

- Access to vault cash and coin is restricted to an individual assigned to the cash or under dual control
- Teller and vault cash limits are monitored at the branch level and cash balances in excess of established limits are approved.
- Access to teller cash is restricted to the individual tellers assigned to the cash.
- Teller and vault cash differences are monitored, investigated and reported to management in accordance with the institution's established limits and parameters.
- Cash shipments and receipts are verified under dual control.
- Transfers of cash between branches are performed by a bonded messenger or independent courier service. Logs are maintained for all transfers of cash.
- Periodic, surprise teller and vault cash counts are performed by supervisory personnel who do not have routine access to the cash drawers they are counting.
- Each teller balances all cash funds daily.

Cash (Continued)

Audit Procedures

- Discuss with management the process of cash, from initial shipments received at the branch, through access and monitoring to recording the transaction to the general ledger. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Select a sample of tellers during the day and observe cash balances via teller terminals to determine the tellers' adherence to established cash limits during the work day.
- Discuss with management the process for conducting surprise cash counts.
- For all teller cash supplies assigned to the branch (including all teller drawers, cash vault, coin machines, cash recyclers, ATMs, etc.), ensure a properly completed surprise count was performed for the last two required frequency periods (ex. Monthly, Bi-monthly, Quarterly, etc.). Also, test to ensure cash counts were performed on a surprise basis (i.e. not when a teller is out of balance or the same time each month/quarter). Document whether the vault was under sole custody or dual control.

Cash (Continued)

Audit Procedures

- Select a sample of surprise cash counts and test for the following:
 - Cash count was performed by supervisor who was independent of the cash being counted.
 - Cash count was conducted after the teller had balanced to the general ledger (i.e. after any potential outage has been recorded).
 - Cash count included all cash supplies and cash items (returned checks, food stamps, redeemed bonds, etc.) assigned to the teller.
 - Counter physically counted each bill in the teller's possession. For Vault Tellers, the counter should physically count all loose bills and large bills (\$50s and \$100s); sample count strapped \$20s, \$10s, \$5s and \$1s ("fan" straps not counted). For any currency in "Fed wrapped" packages, the counter should open the packages and "fan" bills to ensure legitimacy. For bagged shipments, the counter should either verify the contents or control until pick-up and positively confirm with the receiver. For bagged coin, the counter should "feel" the contents from outside the bag and verify on a sample basis.
 - Counter agreed the cash counted to the teller's records and had the teller sign the cash count form to document the cash was counted with the teller present and the cash had been returned.

Cash (Continued)

Audit Procedures

- Counter agreed the cash counted to the teller's records and had the teller sign the cash count form to document the cash was counted with the teller present and the cash had been returned.
- Counter or independent designee balanced the cash counted back to the general ledger the following day.
- If the teller was counted at any time subsequent to teller balancing (i.e., the teller balanced to the general ledger at 2pm, but the count was performed at 4pm), counter physically verified all post cut-off work (e.g. cashed checks, teller cash transfers, cash in/out tickets).
- On the day following the cash count, counter ensured operations did not make any adjustments to the teller's general ledger cash balance. If an adjustment was made, the individual responsible for balancing the Bank Daily Cash Settlement investigated the adjustment for propriety.
- Counter used the count as an opportunity to determine that other required procedures were being followed (e.g., isolating mutilated currency, properly maintaining bait money, etc.).

Consigned Items

Essential Control Points

- A physical inventory of negotiable and consigned items is performed periodically under dual control or by individuals who do not regularly access the supplies.
- Logs are maintained to record the addition and removal of negotiable and consigned items from the supplies and to record the individuals accessing the supplies.
- Supplies of negotiable and consigned items are restricted to one individual or under dual control.
- The unissued supply of consignment items, including both the working and vault supplies, is periodically reconciled by independent or dual personnel to a consignor's listing. This is typically performed on a quarterly or semi-annual basis.

Audit Procedures

- Discuss with management the process over consigned items, from analysis and authorization, through initiation to recording the transaction to the general ledger. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation. Ensure to include all consignment and related items (Money Orders, Cashiers Checks, Gift Cards, Travelers Checks, Instant Issue Debit Cards, Starter Checks, etc.)

Consigned Items (Continued)

Audit Procedures

- For each negotiable or consignment item (Money Orders, Cashiers Checks, Gift Cards, Travelers Checks, Instant Issue Debit Cards, Starter Checks, etc.) maintained at the branch, review for the following:
 - Access to the reserve supplies of consigned items is restricted to one individual or under dual control.
 - Working supplies of the items are in a drawer or other compartment behind the teller line during business hours and are locked up in the vault at night.
 - Working supplies are assigned to designated individual(s) for accountability.
 - A log is maintained which documents the items sold including the item type, date, teller selling the item, customer/account number, and amount.
 - An individual independent of sales and custody verifies the items sold from the working supply on a daily/weekly basis (trace missing items to sales log to supporting documents).
 - A log is maintained to document additions and removal of items to/from the vault/working supplies and to document the individuals accessing the supplies.

Consigned Items (Continued)

Audit Procedures

- The unissued supply (both working and vault supplies) is periodically (monthly) inventoried by independent or dual personnel (trace items on hand to addition/removal and sales logs).
- The unissued supply (both working and vault supplies) is periodically (monthly) reconciled to consignor's listing or internal master listing by independent or dual personnel (trace items on hand back to consignor or internal master listing).
- 'Delayed Settlement Advises' are received and reviewed by someone independent of check sales and custody (vendor obligation items only).
- For each consigned item maintained at the branch, request the two most recent inventories of consigned items and review for the following:
 - Inventory was performed at least monthly (weekly or quarterly may be appropriate in some instances).
 - Inventory was performed under dual control or by individuals who do not have access to the supplies.

Consigned Items (Continued)

Audit Procedures

- For each consigned item maintained at the branch, request the most recent reconciliation of consigned items and review for the following:
 - Reconciliation was performed at least quarterly.
 - Reconciliation was performed under dual control or by individuals who do not have access to the supplies.
 - Reconciliation was to consignor listings (vendor obligation or issued by vendor) or to a master internal listing (if issued by Bank or Bank obligation).
 - Reconciling items noted were described, dated, and followed through to clearance.

Polling Question #2

Which of the following are essential control points for consigned items?

- A. A physical inventory of negotiable and consigned items is performed periodically under dual control or by individuals who do not regularly access the supplies.
- B. Logs are maintained to record the addition and removal of negotiable and consigned items from the supplies and to record the individuals accessing the supplies.
- C. Supplies of negotiable and consigned items are restricted to one individual or under dual control.
- D. The unissued supply of consignment items, including both the working and vault supplies, is periodically reconciled by independent or dual personnel to a consignor's listing. This is typically performed on a quarterly or semi-annual basis.
- E. All the above.

Nightly Depository

Essential Control Points

- The night depository account opening should be approved by designated and trained personnel. Night depository agreements are in place with customers outlining the terms, responsibilities and individuals authorized to access the night depository bags.
- Processed and unprocessed night depository bags, including cash orders, are returned to customers as authorized by the night depository agreement.
- Night deposits are worked and compared to the deposit tickets and differences are researched, approved by branch personnel and communicated to the customer.
- Night deposits are processed in accordance with the institution's established procedures (i.e., assigned to an individual teller or processed under dual control).
- Access to the night depository is under dual control.



Nightly Depository (Continued)

Essential Control Points

- Bags removed from the night depository are assigned to individual tellers or maintained under joint custody upon removal from the night depository (i.e., bag accountability should be maintained).
- Written contracts are in place with third-party couriers.
- Written agreements exist with night depository customers outlining, at a minimum, processing instructions, individuals authorized to pickup deposits, and how differences should be processed.

Nightly Depository (Continued)

Audit Procedures

- Discuss with management the process over the night depository. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Through inquiry and observation, document the following:
 - Is the night depository maintained under strict dual control?
(**Note:** To be effective, the key and combination can never both be obtained by one individual.)
 - Are completed night deposit contracts, with specimen signatures of authorized personnel, maintained on file for each customer dropping bags?
 - Are certified Corporate or Partnership Resolutions maintained on file for each business contract?
 - Are bags assigned to individual tellers or maintained under joint custody upon removal from the night depository (i.e. bag accountability should be maintained)?
 - Are controls established over removal and assignment of responsibility for processing the deposit? (Note: Bank procedures may require someone to document witnessing the processing of the deposit.)

Nightly Depository (Continued)

Audit Procedures

- Are authorized signatures required for receiving unprocessed bags? (Note: An Unprocessed bag is open the branch holds and does not open until the customer comes in.)
- Are authorized signatures required for receiving processed bags (i.e. only receipt being returned)?
- Are all night deposit bags individually listed on a log sheet?
- Are signatures/initials of processing and releasing tellers noted on the night deposit log?
If the bag is processed, is the amount of cash deposited noted on the log sheet?
- Select a sample of days and review the night depository logs for evidence of the following:
- Log documented that the night depository was opened under dual control.
(Refer to the listing of key and combination holders to determine if dual control existed.)
- Number of bags/envelopes removed from the night depository agreed to the detail of listed bags/envelopes processed.

Nightly Depository (Continued)

Audit Procedures

- If required by Bank policy, a witness signed the log documenting dual processing of the deposit.
- Bags were documented as “processed” or “returned unprocessed” with a customer signature and Bank employee initial
- Select a sample of accounts for which customers drop bags in the night depository. Determine if a properly completed night deposit agreement is on file for the customer. Determine if a properly completed corporate resolution is on file, if applicable, and the customer signing the night deposit agreement is authorized by the corporate resolution.
- Obtain the receipts or logs showing night depository bags returned with cash orders. Select a sample and determine whether bags were returned to an authorized individual by reviewing the night depository agreement and/or list of authorized agents provided by the customer.

Physical Security

Essential Control Points

- Branch opening procedures are in place to help prevent an ambush robbery.
- Employees are knowledgeable of the institution's security procedures including branch opening procedures and security inspections.
- Duplicate keys and combinations are maintained under dual control.
- Teller, vault, ATM cash and customer deposits in the ATM and night depository are physically safeguarded.
- Surveillance equipment is used to monitor and record the branch and ATM activities.

Audit Procedures

- Discuss with management the process over physical security. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.

Physical Security (Continued)

Audit Procedures

- Discuss with management the process over physical security. Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Through observation, determine whether teller workstations, vaults, ATM and night depository are equipped with lockable drawers and/or with safes, camera activation buttons, and alarm systems.
 - Teller cash supplies should be under the restricted control of an assigned teller (i.e. no one else can individually gain access).
 - Vault cash should be maintained under dual control. If vault cash is assigned to a head or lead teller, then the cash should only be accessible by that teller and be surprise cash counted along with their teller drawer and other cash supplies
- Through observation, determine whether access to behind the teller line is restricted to authorized personnel. Determine whether access to the teller line is restricted by locked gates or doors.

Physical Security (Continued)

Audit Procedures

- Through inquiry and observation, determine whether cash vaults and teller drawers are required to have bait money and/or dye packs. If bait money is utilized, determine whether a current listing of bait money by serial number and denomination is maintained.
- Through inquiry, determine whether locks/combinations to the institution doors and vaults are changed when a key employee terminated employment or transferred to another location with the institution.
- Through inquiry and observation, determine if duplicate keys and combinations are maintained under dual control. Also, determine if a key and combination log exists that lists the keys and combination that has been given to each employee and that this log is updated on a regular basis to reflect current employees.

Physical Security (Continued)

Audit Procedures

- Through inquiry, determine if branch opening/closing security procedures have been established for all branch locations.
 - In order to prevent an ambush robbery, branch opening procedures should specify that the first person to enter the branch should, after inspecting the interior, exit the building and signal for the second employee to enter. Also, the all-clear signal should not be set until after the second employee has entered the building and verified that the branch is clear.
 - Vaults should be locked by dual personnel. A log should be maintained that documents which individual shut the door, set the lock/alarm, and set the vault timer and also the individual who checked to ensure the door was closed, the lock was set, and the vault timer was set appropriately.
- Observe morning opening procedures and determine if they are adequate to reduce the likelihood of an ambush robbery.
- In order to prevent an ambush robbery, branch opening procedures should specify that the first person to enter the branch should, after inspecting the interior, exit the building and signal for the second employee to enter. Also, the all-clear signal should not be set until after the second employee has entered the building and verified that the branch is clear.

Physical Security (Continued)

Audit Procedures

- Through observation, determine whether institution and ATM activity is monitored by surveillance equipment (i.e., video or digital). Determine whether the following controls exist over surveillance equipment:
 1. Associated digital surveillance equipment or video recorders and monitors are maintained in a restricted area accessible to authorized individuals only.
 2. Cameras cover all branch exits, teller positions and ATM locations.
 3. Equipment is periodically tested, and maintenance is regularly performed to assure proper functioning.
 4. Retention schedules of digital records or video tapes are maintained and followed.

Safe Deposit Box

Essential Control Points

- Customers are notified of delinquent safe deposit box rental payments and forced openings.
- Access to the contents of abandoned or deceased customer-owned safe deposit boxes is restricted under dual control.
- Customer identity is verified prior to allowing access to safe deposit boxes.
- Safe deposit boxes are flagged or marked for delinquent payments or the death of customers.
- Access to the safe deposit box area is restricted.
- Access to keys to safe deposit boxes owned by the institution (i.e., unissued boxes and boxes used by the institution) is restricted to a single individual or under dual control.
- Locks are changed on safe deposit boxes where keys have not been surrendered prior to renting the box to another customer.
- Safe deposit box contracts are in place with customers outlining the terms, responsibilities and individuals authorized to access the safe deposit box. The safe deposit box account opening should be approved by designated and trained personnel.

Safe Deposit Box (Continued)

Essential Control Points

- The input of safe deposit box customer information and rental income is reviewed for accuracy. The review should be performed by an individual who does not have access to or responsibility for recording transactions to the safe deposit box subsidiary ledger.
- The contents of drilled safe deposit boxes are handled in accordance with regulatory requirements (i.e., escheatment).
- Permanent records are maintained for all vault entries, including customers' signatures, dates and times of entry, and safe deposit box custodian initials.

Safe Deposit Box (Continued)

Audit Procedures

- Discuss with management the process over safe deposit boxes. Document whether the controls below are in place:
 - Permanent records kept for all vault entries, including customers' signatures, dates and times of entry and exit, and safe deposit custodian initials maintained.
 - Legal documents relating to safe deposit boxes (e.g. contracts) obtained from customers.
 - Safe deposit custodian compares customer signatures for entry into safe deposit boxes to the contract or other independent document.
 - Locks are changed for surrendered safe deposit boxes (at least whenever both keys are not returned).
 - Dual control of keys is maintained for surrendered and available safe deposit boxes.
 - Controls over the guard key to safe deposit boxes is adequate to prevent unauthorized access.
 - Procedures established to notify customers upon delinquent payment status.
 - Controls established to ensure regulatory procedures (i.e.. escheatment) are followed upon drilling safe boxes and removing contents.

Safe Deposit Box (Continued)

Audit Procedures

- Rented and un-rented boxes reconciled between subsystem reports and the general ledger.
- Procedures require the safe deposit boxes to be either locked “open” or “closed” when the customer tin is removed (i.e. the lock is engaged with the door either open or closed and both the customer's key and the safe deposit custodian's key are required to return the tin and secure the box)? (Note: If possible, the auditor should observe this procedure.)
- Document the process, considering the essential control points. Comment on whether the controls are designed effectively and are in operation.
- Obtain a listing of delinquent accounts from the subsidiary ledger. Select a sample of accounts > 30 days past due (or the criteria used by the institution) and determine whether customers were notified. For accounts > 90 days past due (or the criteria used by the institution), determine whether the customer has been notified that the box will be drilled. Observe that the safe deposit boxes have been flagged or marked as delinquent.

Safe Deposit Box (Continued)

Audit Procedures

- Select a sample of recent safe deposit box entries and test for the following:
 1. Permanent records are kept for all vault entries, including customers' signatures, dates and times of entry.
 2. Safe deposit custodian initials are maintained.
 3. Legal documents relating to safe deposit boxes (i.e., contracts) are obtained from customers.
 4. Access is gained by an authorized signor only.

Safe Deposit Box (Continued)

Audit Procedures

- Interview applicable bank management and document whether the controls below are in place and document the bank's current branch procedures.
 1. Are safekeeping items maintained under dual control?
 2. Are pre-numbered receipts given to customers when safekeeping items are received?
 3. Does someone independent review unissued pre-numbered receipts to ensure numeric sequence?
 4. Are customers required to sign for returned safekeeping items (either in person or via certified mail receipt)?
 5. Are periodic (monthly or quarterly) inventories performed by independent or dual personnel? (Note: The inventory should include a comparison of items on hand to outstanding receipts.)

Regulatory Disclosures

Essential Control Points

- Funds Available Disclosure should be visible where deposits are taken (Required if the ATM accepts deposits. Not required for the drive-thru and night depository).
- FDIC Notice should be visible at each teller station, including drive thru, but not required at ATM and night depository.
- Notice of availability for the bank's HMDA analysis should be visible to lobby traffic (only required if the branch is in an MSSA).
- Fair Housing Poster should be visible to lobby traffic.
- In accordance with the ADA, the branch should have a designated parking place, a curbside ramp for access to the entrance, lowered buttons for elevators, and other applicable accommodations.
- The branch's non-deposit investment products should be sold in a separate area of the branch and be clearly identified as not being FDIC insured.

Regulatory Disclosures (Continued)

Audit Procedures

- Through observation, determine whether the following regulatory notices are properly displayed.
 1. Funds Available Disclosure (Should be visible where deposits are taken. Required if the ATM accepts deposits. Not required for the drive-thru and night depository.)
 2. FDIC Notice (Should be at each teller station, including drive thru, but not required at ATM and night depository)
 3. Notice of availability for the bank's HMDA analysis (Should be visible to lobby traffic; only required if the branch is in an MSSA)
 4. Fair Housing Poster (Should be visible to lobby traffic)
- Through observation, determine accessibility for physically impaired customers is provided. For example, the branch should have a designated parking place, a curbside ramp for access to the entrance, lowered buttons for elevators, etc.
- Through observation and inquiry determine whether non-deposit investment products are sold in a separate area of the branch and are clearly identified as not being FDIC insured.

Hold Mail

Essential Control Points

- Hold mail statements are stored under dual control.
- Written procedures exist for the handling of hold mail statements.
- Customers are required to sign a log when retrieving hold mail statements.

Audit Procedures

- Interview applicable bank management and document whether the controls below are in place and document the bank's current branch procedures.
 1. Are hold mail agreements required for all customers requesting hold mail?
 2. Is customer hold mail maintained under restricted control by someone other than a teller?
 3. Are hold mail statements logged onto a branch record (e.g. a log sheet or customer access record) prior to customer pick-up?
 4. Are authorized individuals required to sign when picking up hold mail? (Note: See test below.)
If hold mail statements are not picked up for a specified amount of time (ex. 30 days or two statement cycles), are they mailed to the customer?



Hold Mail (Continued)

Audit Procedures

- Obtain a listing or system report of all mail (account statements) held within the branch. Select a sample of accounts and ensure a hold mail agreement is on file.
- Obtain the pick-up logs for the branch's hold statements. Determine whether the statements were released to a person authorized in the hold mail agreement.



Polling Question #3

Following this session, do you have a better understanding of how conduct an audit over the branch operations function?

- A. Yes
- B. Somewhat
- C. Not really



Pandemic Regulatory Guidance Considerations

Presented by Layne McGuire



Regulator Guidance

- Interagency Examiner Guidance For Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Institutions
- 2020 Interagency Statement on Pandemic Planning
- Joint Statement on Additional Loan Accommodations Related to COVID-19



Interagency Examiner Guidance For Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Institutions

SR 20-15

June 23, 2020



Polling Question #1

How knowledgeable are you of pandemic-related regulatory guidance?

- A. Very knowledgeable
- B. Fairly knowledgeable
- C. Only slightly knowledgeable
- D. Huh?



SR 20-15

- Examiners will consider **the unique, evolving, and potentially long-term nature of the issues confronting institutions and exercise appropriate flexibility in their supervisory response. Stresses caused by COVID-19** can adversely impact an institution's financial condition and operational capabilities, even when institution management has appropriate governance and risk management systems in place to identify, monitor, and control risk



SR 20-15

- Many institutions have also materially modified operational processes to continue providing products and services while adhering to stay-at-home and social distancing guidelines. These modifications, including extensive use of work-at-home strategies and the need to quickly implement various stimulus programs, may have stressed change management processes. **Operational, compliance, and cyber risks may increase for many institutions, and internal controls may need to evolve as risks and operations change.**



SR 20-15

- Examiners should assess **the reasonableness of management's actions in response to the pandemic given the institution's business strategy and operational capacity** in the distressed economic and business environment in which the institution operates. When assigning the composite and component ratings, examiners will review management's assessment of risks presented by the pandemic, considering the institution's size, complexity, and risk profile.
- An examiner's assessment **may result in downgrading component or composite ratings for some institutions.**

SR 20-15

- When considering whether to take a formal or informal enforcement action in response to issues related to the pandemic, **the agencies will consider whether an institution's management has appropriately planned for financial resiliency and continuity of operations; implemented prudent policies; and is pursuing realistic resolution of the issues confronting the institution.**
- Examiners should evaluate **management's initial and ongoing assessment of the risk that the pandemic presents** to the institution.

SR 20-15

- The risks associated with the COVID-19 pandemic, as well as impacts of policy responses, can be challenging to assess in real time. Examiners will **assess an institution's risk identification and reporting processes** given the level of information available and stage of local economic recovery.
- Examiners should determine **whether an institution's assessment of risk is sufficient in scope and content**. In reviewing the assessments, examiners should recognize that the issues confronting institutions are complex, evolving, and may involve protracted resolution.



SR 20-15

- The agencies have encouraged institutions to use their capital buffers to promote lending activities and other financial intermediation activities in a safe and sound manner.
- Examiners will evaluate capital relative to the nature and extent of the institution's risks.
- Examination scopes may need to be adjusted to reflect the significance of affected loan and investment portfolios. Examiners **will continue to assess credits in line with the interagency credit classification standards, while recognizing the constraints posed by the pandemic.**

SR 20-15

- Examiners will assess management's ability to implement **prudent credit modifications and underwriting**, maintain appropriate loan risk ratings, designate appropriate accrual status on affected loans, and provide for an appropriate Allowance for Loan and Lease Losses (ALLL) or Allowances for Credit Losses (ACLs), as applicable.
- The assessment of each loan should be based on the **fundamental characteristics** affecting the collectability of that particular credit.

SR 20-15

- Examiners will recognize that the rapidly changing environment and limited operational capacity **may temporarily affect the institution's ability to meet normal expectations of loan review** (e.g. schedule or scope of reviews). Examiners will assess the institution's support for any delays or reductions in scope of credit risk reviews and consider management's plan to complete appropriate reviews within a reasonable amount of time.
- Regarding new loans, examiners will assess the appropriateness of the institution's underwriting standards. Examiners should assess underwriting by reviewing **a sample of loans originated during or after the pandemic.**

SR 20-15

- The agencies view the PPP as an important program to help institutions continue to lend to customers in need, without exposing the institution to credit risk, so long as the institution follows SBA's program guidelines. Moreover, in assessing an institution's safety and soundness, **examiners will not criticize institutions that participate in the PPP in accordance with SBA program guidelines.**

SR 20-15

- Examiners should assess the appropriateness of an institution's **policies and procedures for credit renewals, extensions, or modifications.**
- In assessing an institution's loan modification practices, examiners will review loan modifications to evaluate whether management is applying **appropriate loan risk grades** and making appropriate accrual status decisions on loans affected by the pandemic.

SR 20-15

- Institutions may allow **borrowers affected by the pandemic to defer payment** of principal, interest, or both for a reasonable period with the expectation that the borrower will resume payments in the future. The Revised Interagency Statement indicates that during the short-term arrangements, **these loans generally should not be reported as nonaccrual**. As information becomes available indicating repayment of a specific loan or accrued interest is in doubt, examiners should review institution practices against appropriate charge-off guidance regarding accrued interest and principal.

SR 20-15

- Examiners should review an institution's methodology for calculating the ALLL or ACLs, as applicable. In assessing whether the ALLL or ACLs are appropriate, examiners will assess whether management has considered **relevant available information about the collectability of the institution's loan portfolio**, along with any changes to the institution's lending practices and economic conditions as a result of the pandemic.
- Examiners should understand that management may need to consider **qualitative adjustments** to credit loss estimates for information not already captured in the loss estimation process.

SR 20-15

- Examiners should confirm that institutions monitor their risk exposures in **municipal bonds** to assess whether those bonds continue to be the credit equivalent of an investment grade security and are appropriately classified, consistent with the interagency credit classification standards.
- For existing and new real estate loans, examiners should assess the institution's policies and practices for **valuing collateral** in real estate markets that have experienced a substantial, but possibly temporary, change in real estate values as a result of pandemic containment measures.

SR 20-15

- The agencies have **temporarily allowed supervised financial institutions to defer obtaining an appraisal or evaluation for up to 120 days after the closing** of residential and commercial real estate loans (other than loans for acquisition, development, and construction of real estate). Examiners should evaluate whether an institution is making best efforts to obtain a credible valuation of real property collateral before the loan closing and how any backlog of appraisals or evaluations is being addressed.

SR 20-15

- As part of the institution's risk management assessment, examiners will evaluate institution management based on the **reasonableness of management's response to the pandemic**. As additional information becomes available, examiners expect management to update risk assessments, measure the effectiveness of its response, and adjust, as necessary.
- Examiners will evaluate institution management on its ability to properly **identify and prudently manage risks** associated with the pandemic.



SR 20-15

- **Rapid changes in operational processes and increasing fraud and cyber threats may result in a heightened operational risk environment.** Examiners will review the steps management has taken to assess and implement effective controls for new and modified operational processes. Examiners will assess actions management has taken to adapt fraud and cybersecurity controls to manage heightened risks related to the adjusted operating environment. Examiners will also review how management has assessed institutions' third parties' controls and service delivery performance capabilities post crisis.

SR 20-15

- Examiners will consider how **COVID-19-related responses may impact plans and schedules for internal audit and independent risk management reviews**, including the need to incorporate audits or reviews of new operational processes and programs.
- In addition, examiners should **review risk management and audit monitoring of programs to support consumers and businesses such as PPP**, mortgage deferrals, loan forbearance, and other new programs that may pose credit, legal, and compliance risks if not properly managed.

SR 20-15

- When assessing earnings, examiners will evaluate how institutions are **accounting for and estimating allowances for accrued interest from modified loans**, as applicable, in accordance with GAAP and Call Report instructions.
- This assessment should consider the adequacy and reasonableness of any **revisions to the institution's budget and strategic plan**, including projections from participation in government programs related to the pandemic.



SR 20-15

- There remains **considerable uncertainty around the impact of COVID-19 on liquidity profiles**. Examiners will consider the nature and timing of pandemic-related inflows and outflows when reviewing the adequacy of an institution's liquidity and be cognizant of how management is employing any influx of liquid resources.
- Examiners will **not criticize** an institution for appropriate use of the discount window or other Federal Reserve lending programs



SR 20-15

- Examiners should determine whether management has procedures for **reviewing and updating its asset and liability management models** for any unusual fluctuations in deposit balances, adjustments to loan payments, changes in interest rates, and other modifications to ensure the integrity, accuracy, and reasonableness of the models.



2020 Interagency Statement on Pandemic Planning

Update to the 2007 Interagency Statement on Pandemic Planning

August 2020



Interagency Statement on Pandemic Planning

- This guidance is an **update to the 2007 Interagency Statement on Pandemic Planning as well as the “Interagency Advisory on Influenza Pandemic Preparedness” issued on March 15, 2006** by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as well as the “Letter to Credit Union 06-CU-06 - Influenza Pandemic Preparedness” issued by the National Credit Union Administration in March 2006.



Interagency Statement on Pandemic Planning

- This guidance identifies actions that financial institutions should take to **minimize the potential adverse effects of a pandemic**. Specifically, the institution's business continuity plan(s) (BCP) should address pandemics and provide for **a preventive program, a documented strategy scaled to the stages of a pandemic outbreak, a comprehensive framework** to ensure the continuance of critical operations, a testing program, and an oversight program to ensure that the plan is reviewed and updated.



Interagency Statement on Pandemic Planning

- There are **distinct differences between pandemic planning and traditional business continuity planning**. When developing business continuity plans, financial institution management typically considers the effect of various natural or man-made disasters that may differ in their severity. These disasters may or may not be predictable, but they are usually short in duration or limited in scope.
- Pandemic planning **presents unique challenges to financial institution management**. Unlike natural disasters, technical disasters, malicious acts, or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration.



Interagency Statement on Pandemic Planning

- Pandemic plans should be **sufficiently flexible to effectively address a wide range of possible effects that could result from a pandemic**. Pandemic plans need to reflect the institution's size, complexity, and business activities. The potential impact of a pandemic on the delivery of a financial institution's critical financial services should be incorporated into the ongoing business impact analysis and risk assessment processes.
- The institution's BCP should then be revised, if needed, to reflect **the conclusions of its business impact analysis and risk assessment**.



Interagency Statement on Pandemic Planning

To address the unique challenges posed by a pandemic, the financial institution's BCP should provide for:

1. A **preventive program to reduce the likelihood that an institution's operations** will be significantly affected by a pandemic event, including: monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers, in addition to providing appropriate hygiene training and tools to employees.

Interagency Statement on Pandemic Planning

To address the unique challenges posed by a pandemic, the financial institution's BCP should provide for:

2. A **documented strategy** that provides for scaling the institution's pandemic efforts, so they are consistent with the effects of a particular stage of a pandemic outbreak, such as the 6 intervals described by the Center for Disease Control and Prevention (CDC):
(<https://www.cdc.gov/flu/pandemic-resources/national-strategy/intervals-framework.html>).

The strategy will also need to outline plans describing how to recover from a pandemic wave and proper preparations for any following wave(s).

Interagency Statement on Pandemic Planning

To address the unique challenges posed by a pandemic, the financial institution's BCP should provide for:

3. A comprehensive framework of facilities, systems, or procedures that provide the organization the capability to continue its critical operations in the event that large numbers of the institution's staff are unavailable for prolonged periods. Such procedures could **include social distancing to minimize staff contact, telecommuting, redirecting customers from branch to electronic banking services, or conducting operations from alternative sites.**



Interagency Statement on Pandemic Planning

To address the unique challenges posed by a pandemic, the financial institution's BCP should provide for:

4. A **testing program** to ensure that the institution's pandemic planning practices and capabilities are effective and will allow critical operations to continue.
5. An **oversight program** to ensure ongoing review and updates to the pandemic plan so that policies, standards, and procedures include up-to-date, relevant information provided by governmental sources or by the institution's monitoring program.



Interagency Statement on Pandemic Planning

Websites to assist in Pandemic Planning:

- <https://www.cdc.gov/flu/pandemic-resources/planning-preparedness/national-strategy-planning.html>
- <http://www.pandemicflu.gov/>.



Interagency Statement on Pandemic Planning

- Traditional business continuity planning and pandemic planning require management to **follow a cyclical process of planning, preparing, responding, and recovering**. However, pandemic planning requires additional actions to identify and prioritize essential functions, employees, and resources within the institution and across other business sectors.
- An institution's **board of directors is responsible for overseeing** the development of the pandemic plan.
- **Senior management is responsible for developing** the pandemic plan and translating the plan into specific policies, processes, and procedures.

Interagency Statement on Pandemic Planning

The potential effects of a pandemic should be a part of the financial institution's overall **Business Impact Analysis** (BIA).

1. **Assess and prioritize essential business functions and processes** that may be affected by a pandemic;
2. Identify **the potential impact of a pandemic** on the institution's essential business functions and processes, and supporting resources;
3. Identify the **potential impact of a pandemic on customers**: those that could be most affected and those that could have the greatest impact on the (local) economy;

Interagency Statement on Pandemic Planning

The potential effects of a pandemic should be a part of the financial institution's overall Business Impact Analysis (BIA).

4. Identify the **legal and regulatory requirements** for the institution's business functions and processes;
5. Estimate the **maximum downtime** associated with the institution's business functions and processes that may occur during a pandemic;
6. Assess **cross training conducted for key business positions** and processes; and
7. Evaluate the **plans of critical service providers** for operating during a pandemic.



Interagency Statement on Pandemic Planning

- A key part of an institution's BIA that addresses pandemics is to **examine external factors**. For example, assessing the impact of critical interdependencies will involve making planning assumptions regarding the availability of external services and prioritizing the effect of possible disruptions. In addition, potential travel restrictions imposed by health and emergency management officials may limit access to those services, even if they are still operating.

Interagency Statement on Pandemic Planning

Important risk assessment and risk management steps that are important for pandemic planning include:

- Prioritizing the **severity of potential business disruptions** resulting from a pandemic, based on the institution's estimate of impact and probability of occurrence on operations;
- Performing a **“gap analysis”** that compares existing business processes and procedures with what is needed to mitigate the severity of potential business disruptions resulting from a pandemic;
- Developing a **written pandemic plan** to follow during a possible pandemic event;
- **Reviewing and approving the pandemic plan** by the board or a committee thereof and senior management at least annually; and
- **Communicating and disseminating the plan** and the current status of the pandemic to employees.



Interagency Statement on Pandemic Planning

Specific risk assessment and risk management actions arising from a pandemic include the following:

- **Third Parties** - Open communication and coordination with third parties, including critical service providers, is an important aspect of pandemic planning.
- **Identification of Triggering Events** - A triggering event occurs when an environmental change takes place that requires management to implement its response plans based on the pandemic alert status.

Interagency Statement on Pandemic Planning

Specific risk assessment and risk management actions arising from a pandemic include the following:

- **Employee Protection Strategies** - Employee protection strategies are crucial to sustain an adequate workforce during a pandemic.
- **Mitigating Controls** - Despite the unique challenges posed by a pandemic, there are control processes that management can implement to mitigate risk and the effects of a pandemic.
- **Remote Access** - During a pandemic there may be a high-reliance on employee telecommuting, which could put a strain on remote access capabilities such as capacity, bandwidth, and authentication mechanisms.



Interagency Statement on Pandemic Planning

Risk **monitoring and testing** of the pandemic plan is important to the overall planning process. A robust program should incorporate testing:

- **Roles and responsibilities** of management, employees, key suppliers, and customers;
- Key pandemic planning **assumptions**;
- Increased reliance on online banking, telephone banking, and call center services; and
- **Remote access and telecommuting capabilities.**

Polling Question #2

Pandemic-related regulatory guidance includes which of the following?

- A. Interagency Examiner Guidance For Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Institutions
- B. 2020 Interagency Statement on Pandemic Planning
- C. Joint Statement on Additional Loan Accommodations Related to COVID-19
- D. All the above.



Joint Statement on Additional Loan Accommodations Related to COVID-19

August 3, 2020



Additional Loan Accommodations

- The COVID event has had a significant adverse impact on consumers, businesses, financial institutions, and the economy. To address such impacts, the Coronavirus Aid, Relief, and Economic Security Act (**CARES Act**) provides several forms of relief to businesses and borrowers, and some states and localities have provided similar credit accommodations. Also, many financial institutions have voluntarily offered other credit accommodations to their borrowers.
- The FFIEC members have encouraged financial institutions to work **prudently with borrowers** who are or may be unable to meet their contractual payment obligations because of the COVID event.



Additional Loan Accommodations

- The FFIEC members encourage financial institutions to consider **prudent accommodation options** that are based on an understanding of the credit risk of the borrower; are consistent with applicable laws and regulations; and, that can ease cash flow pressures on affected borrowers, improve their capacity to service debt, and facilitate a financial institution's ability to collect on its loans.
- **Imprudent practices can adversely affect borrowers and expose financial institutions** to increases in credit, compliance, operational, and other risks as well as present risks to a financial institution's capital.



Additional Loan Accommodations

The following principles provide prudent practices for financial institutions to work with borrowers in a safe and sound manner as loans near the end of accommodation periods.

- **Prudent Risk Management Practices** - Prudent risk management practices include identifying, measuring, and monitoring the credit risks of loans that receive accommodations. Sound credit risk management includes applying appropriate loan risk ratings or grades and making appropriate accrual status decisions on loans affected by the COVID event.



Additional Loan Accommodations

The following principles provide prudent practices for financial institutions to work with borrowers in a safe and sound manner as loans near the end of accommodation periods.

- **Well-Structured and Sustainable Accommodations** - For a borrower that continues to experience financial challenges after an initial accommodation, it may be prudent for the financial institution to consider additional accommodation options to mitigate losses for the borrower and the financial institution.



Additional Loan Accommodations

The following principles provide prudent practices for financial institutions to work with borrowers in a safe and sound manner as loans near the end of accommodation periods.

- **Consumer Protection** - Financial institutions are encouraged to provide consumers with available options for repaying any missed payments at the end of their accommodation to avoid delinquencies or other adverse consequences. Financial institutions are also encouraged, where appropriate, to provide consumers with options for making prudent changes to the terms of the credit product to support sustainable and affordable payments for the long term.



Additional Loan Accommodations

The following principles provide prudent practices for financial institutions to work with borrowers in a safe and sound manner as loans near the end of accommodation periods.

- **Accounting and Regulatory Reporting** - Financial institutions must follow applicable accounting and regulatory reporting requirements for all loan modifications, as the term “modification” is used in U.S. generally accepted accounting principles (GAAP) and regulatory reporting instructions, including additional modifications made to borrowers who may continue to experience financial hardship at the end of the initial accommodation period



Additional Loan Accommodations

The following principles provide prudent practices for financial institutions to work with borrowers in a safe and sound manner as loans near the end of accommodation periods.

- **Internal Control Systems** - Prudent risk management practices at the end of initial accommodation periods and for additional accommodations include quality assurance, credit risk review, operational risk management, compliance risk management, and internal audit functions that are commensurate with the size, complexity, and risk of the financial institution's activities.

Additional Loan Accommodations

Prudent **testing by internal control functions** typically confirm the following:

- Accommodation terms are extended with **appropriate approval**;
- Additional accommodation options offered to borrowers are presented and processed in **a fair and consistent manner** and comply with applicable laws and regulations, including fair lending laws;
- Servicing systems **accurately consolidate balances, calculate required payments, and process billing statements** for the full range of potential repayment terms that exist once the accommodation periods end;



Additional Loan Accommodations

Prudent testing by internal control functions typically confirm the following:

- Staff, including problem loan and collections personnel **are qualified** and can efficiently handle expected workloads;
- Borrower and guarantor communications, and legal documentation, are **clear, accurate, and timely**, and in accordance with contractual terms, policy guidelines, and federal and state laws and regulatory requirements; and
- **Risk rating assessments are timely and appropriately supported.**



Small Group Activity

In your Small Group, discuss Pandemic-specific changes that your bank has made/is making to address customer and or employee concerns. These changes can be accommodations made to customers/employees, new deposit or loan programs, branch operations, etc.

- List at least 5 specific changes banks in your group have made.
- Select a spokesperson to report 1 of the changes to the entire Class.



Polling Question #3

Following this session, do you have a better understanding of pandemic-related regulatory guidance?

- A. Yes
- B. Somewhat
- C. Not really



FDICIA/SOX Compliance

Presented by Sarah Schwartz



Topics

- What the Regulators Think
- External Auditor Requirements
- Internal Audit/Management Requirements
- Crowe's FDICIA/SOX Compliance Approach
- Managing the Data
- Conclusions and Questions

Polling Question #1

How comfortable are you when it comes to the topic of FDICIA/SOx Compliance?

- A. Very comfortable
- B. Fairly comfortable
- C. Only slightly comfortable
- D. What is FDICIA and SOx?



What the Regulators Think



FDICIA- The Regulatory Environment

- Revised FDIC Part 363 Guidance and attestation standards (AT 501) bring FDICIA regulatory expectations internal control reporting and audit requirements more in line with what is required under SOx 404 and AS 5.
- Overall, higher level of scrutiny of entire FDICIA process



External Auditor Requirements

AT 501 / SSAE 15 - ICOFR

	Publicly held companies that are accelerated filers	Nonaccelerated filers - public banks with assets of \$1 billion or more	Private banks with assets of \$1 billion or more
Auditing Standard for audits of internal control over financial reporting	PCAOB AS5	SSAE 15 ³	SSAE 15
Management guidance for internal control over financial reporting	SEC interpretive guidance and most commonly the COSO Framework	SEC interpretive guidance and most commonly the COSO Framework	FDIC regulations / guidance and most commonly the COSO Framework

AT 501 / SSAE 15 - ICOFR

- AICPA's Auditing Standards Board has issued Statement on Standards for Attestation Engagements No. 15 "An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements"
 - **SSAE No. 15 Replaces AT501**
 - Effective Dec. 15, 2008
 - Substantial convergence with PCAOB Auditing Standard No. 5 (AS5)



SSAE 15

- Potential significant changes for management from what was required under old AT 501 standard
 - **Documentation** and evaluation of key controls
 - Use of COSO 2013 framework
 - Performance of walk-throughs
 - Evaluation of deficiencies



SSAE 15

Some key provisions:

- New definitions for significant deficiency and material weakness
- Defines role of risk assessment – focus on areas of highest risk
- Addressing the risk of fraud when planning an examination of internal controls
- Top-down approach: beginning at Financial Statement level and focusing on entity-level controls



SSAE 15

Some key provisions (cont.):

- The ability to use the work of others, such as internal auditors and third parties
- Selecting and testing controls – including design evaluation, the timing and extent of control testing, and the incorporation of knowledge obtained in subsequent years' examinations
- Evaluating the severity of identified deficiencies
- Highlighting indicators of material weaknesses



FDICIA Part 363

- SSAE 15 now applies for all banks over \$1 billion in assets (public banks use SOx 404 / AS 5)
- FDICIA was the model for SOx 404: non-bank entities look to banking ICOFR models for best practices
 - Bank regulators provide guidance in examination manuals and supervision letters



FDICIA - Part 363

External auditor independence.

The external auditor must comply with the independence standards and interpretations of the American Institute of Certified Public Accountants, the Securities and Exchange Commission, and the Public Company Accounting Oversight Board (PCAOB). If the standards differ, the auditor must comply with the more restrictive rule.

External auditor work paper retention.

The final rule establishes retention requirements for the external auditor's working papers to be consistent with the seven-year retention period applicable to auditors of public companies.



FDICIA - Part 363

Peer reviews and inspection reports.

Within 15 days of receiving notification that either a peer review has been accepted or a PCAOB inspection report has been issued or before commencing any work, whichever is earlier, the external auditor must file with the FDIC two copies of the most recent peer review report and the public portion of the most recent PCAOB inspection report, if any, accompanied by any letters of comment, response, and acceptance.



Audit Committee / Management Requirements

AT 501 / SSAE 15 - ICOFR

	\$500 million to \$1 billion in assets, as measured at the beginning of the fiscal year	\$1 billion or more in assets, as measured at the beginning of the fiscal year
Part 363 Annual Reporting (due within 120 days after the end of the institution's fiscal year-end)	Audited financial statements	Audited financial statements
	Statement of management's responsibilities	Statement of management's responsibilities
	Management's assessment of compliance with designated safety and soundness laws and regulations	Management's assessment of compliance with designated safety and soundness laws and regulations
		Assessment by management on the effectiveness of internal control over financial reporting
		Attestation by the external auditor on the effectiveness of internal control over financial reporting
Letters and Reports from the External Auditor (due 15 days after receipt)	Any Management letter or other report issued by the external auditor, except for those included in the Part 363 Annual Report	Any Management letter or other report issued by the external auditor, except for those included in the Part 363 Annual Report
Audit Committee Independence	The majority of the audit committee must be independent of management	All of the audit committee must be independent of management



FDICIA - Part 363 – Audit Committees

Duties related to the external auditor.

The final rule specifies that the audit committee's duties include appointing, compensating, and overseeing the external auditor.

Engagement letters with the external auditor.

The audit committee is now required to ensure that the external audit engagement letter does not contain unsafe and unsound limitation of liability provisions.

- The FDIC issued “Interagency Advisory on the Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters” on Feb. 9, 2006, which is available at: www.fdic.gov/news/news/financial/2006/fil06013.html.

FDICIA - Part 363 – Audit Committees

Audit committee independence.

To enhance corporate governance, the FDIC is requiring the Board of Directors to adopt written criteria for evaluating the independence of an audit committee member.

- The final rule provides expanded guidance for Boards of Directors to use in determining independence.
- When assessing an outside director’s relationship with an institution, the Board of Directors should consider the issue not only from the standpoint of the director but also from the standpoint of persons or organizations with which the director is affiliated.
- The final rule provides guidelines to assist boards of directors in fulfilling their responsibility to determine whether existing and potential members of the audit committee are “independent of management.”



FDICIA - Part 363 – Audit Committees

Communications from the external auditor.

Consistent with the requirements of SOX, the final rule requires certain communications by the external auditor to the audit committees, including:

- critical accounting policies;
- alternative accounting treatments discussed with management; and
- written communications provided to management (such as management letters or a schedule of unadjusted differences).



FDICIA - Part 363 - Management

Filing deadlines.

The FDIC has extended the filing deadline for Part 363 Annual Reports by 30 days, so the reports are now due 120 days after the end of the fiscal year. The final rule also changes the procedures for late filings by permitting the use of a 30-day late filing notification for an institution confronted with extraordinary circumstances (which replaces the previously granted 30-day extension).

Compliance with designated laws and regulations.

In addition to the existing requirement for management to state its conclusion regarding compliance with designated safety and soundness laws and regulations, the FDIC has added a requirement to disclose any noncompliance with such laws and regulations.

FDICIA - Part 363 - Management

Illustrative management reports and letters.

The FDIC has provided illustrative management reports and a cover letter in Appendix B of Part 363, although institutions are not required to use the examples. The illustrative management reports and letters include:

- Illustrative Statement of Management's Responsibilities;
- Illustrative Reports on Management's Assessment of Compliance With Designated Laws and Regulations;
- Illustrative Reports on Management's Assessment of Internal Control Over Financial Reporting;
- Illustrative Management Report – Combined Statement of Management's Responsibilities, Report on Management's Assessment of Compliance With Designated Laws and Regulations, and Report on Management's Assessment of Internal Control Over Financial Reporting; and
- Illustrative Cover Letter – Compliance by Holding Company Subsidiaries.



FDICIA - Part 363 - Management

Institutions merged out of existence.

The final rule provides relief from the annual reporting requirements for institutions that are merged out of existence.

Complying at the holding company level.

The final rule will now require the total assets of a holding company's insured depository institution subsidiaries to comprise 75 percent or more of the holding company's consolidated total assets in order for an institution to be eligible to comply with Part 363 at the holding company level.



FDICIA - Part 363 – Management

Internal control framework.

Management and the external auditor are required to identify the internal control framework used to evaluate internal control, which is consistent with the requirement for public companies that are subject to the internal control over financial reporting requirements of SOX.

Disclosure of material weaknesses.

In the final rule, the FDIC has clarified that management must disclose all material weaknesses in internal control over financial reporting that it has identified but have not remedied prior to the end of the institution's fiscal year.

Acquisitions during the year.

The final rule provides relief from the reporting on internal control over financial reporting for businesses acquired during the year.



Polling Question #2

Is FDICIA and/or SOx compliance applicable to your financial institution?

- A. Yes.
- B. No.
- C. Not yet, but soon.
- D. No idea!



Crowe's FDICIA/SOX Compliance Approach

Internal Controls over Financial Reporting for FDICIA/SOX Implementation

- Crowe has met with management of many privately-held financial institutions to discuss the current state of internal control over financial reporting (“ICOFR”). These discussions have related to Sarbanes-Oxley Section 404 and the Federal Deposit Insurance Corporation Improvement Act (“FDICIA”), SAS 130, as well as general discussions as to how financial institutions are addressing their responsibilities for evaluating ICOFR.
- To achieve these general objectives, we suggest financial institutions consider our FDICIA compliance approach, which has been “battle tested” in over 120 financial institutions. This general approach is described in the paragraphs that follow and should provide a general understanding of our suggested implementation methodology.
- Our FDICIA compliance approach is specifically designed to involve the right stakeholders in the project at the right time. This ensures we deliver a solution that meets the needs of management and the external auditor and maximizes efficiency in getting there.



Phase I: Project Planning



Objective

The objective of this phase is to develop the plan to complete the overall project. We believe a well-planned project results in better results by ensuring the right stakeholders are involved from the beginning with clear expectations defined.



Assumptions

- Management will provide list of key stakeholders and members of management.
- Management will help identify areas of risk and processes where critical internal controls over financial reporting reside.



Tasks

- Key Activities
 - Set project scope and approach
 - Confirm buy-in of external auditor
 - Develop overall project plan and timeline

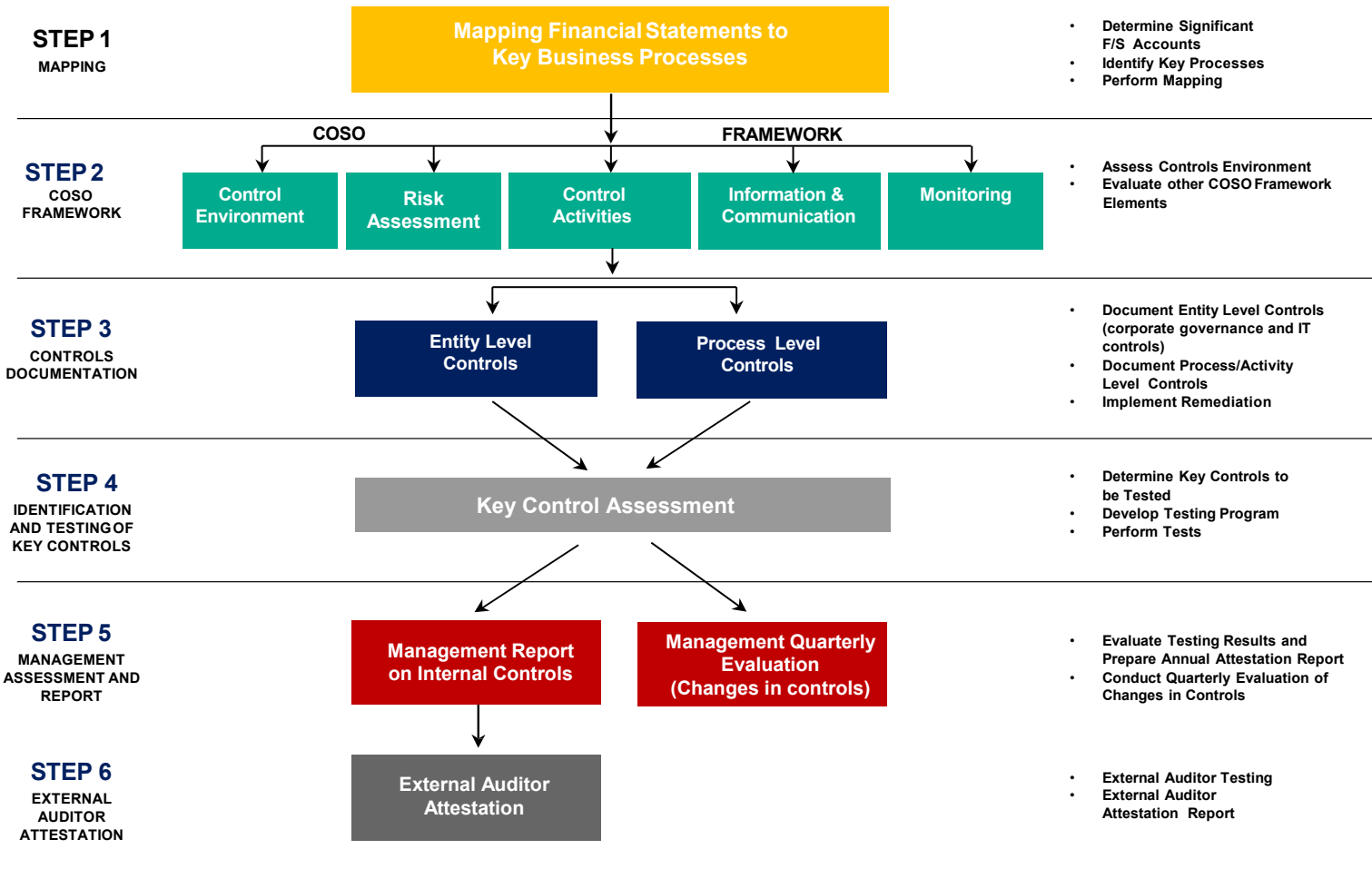


Deliverables

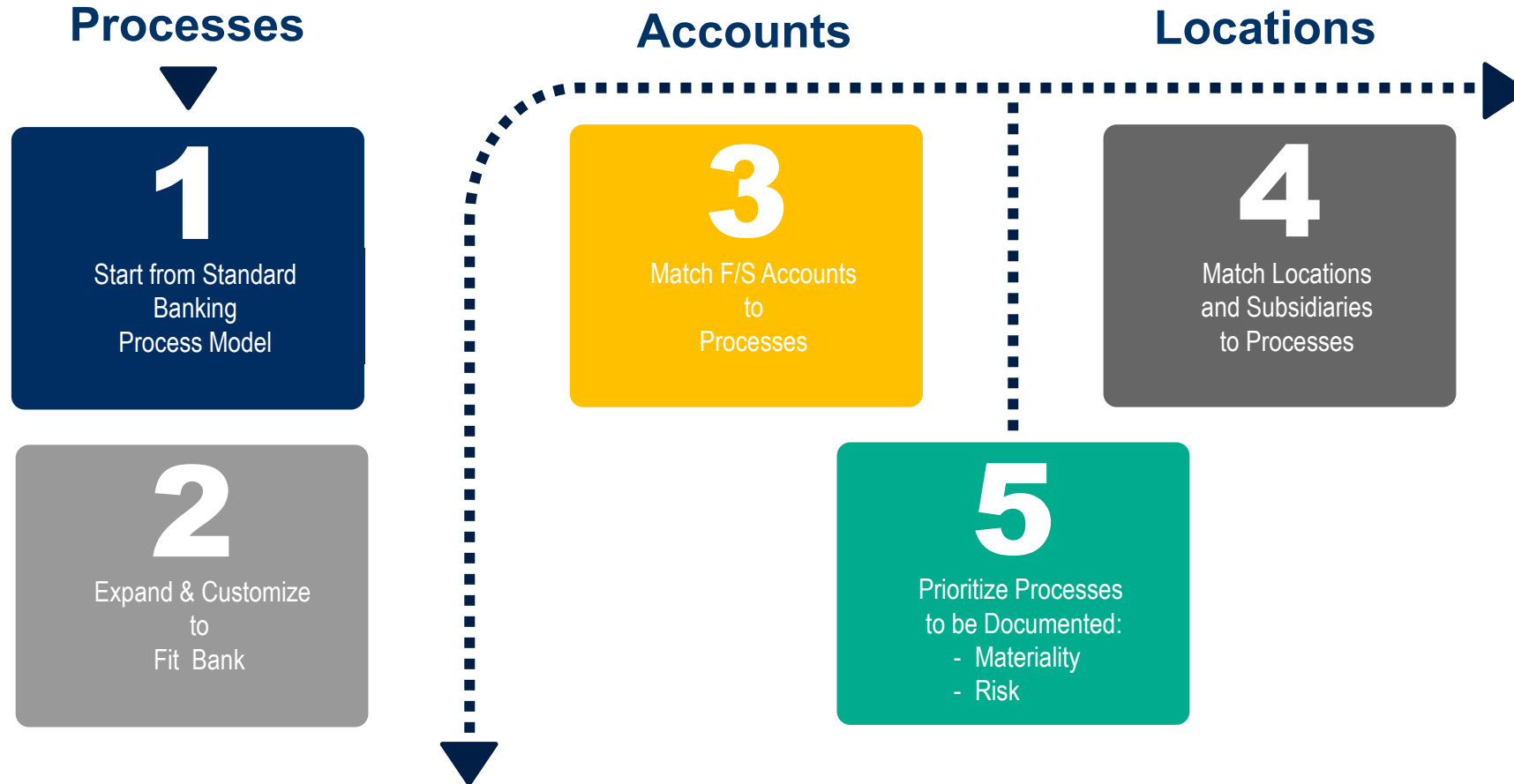
Project planning:

- Overall project plan and timeline
- Mapping matrix of the company's financial statements to key processes throughout the organization.

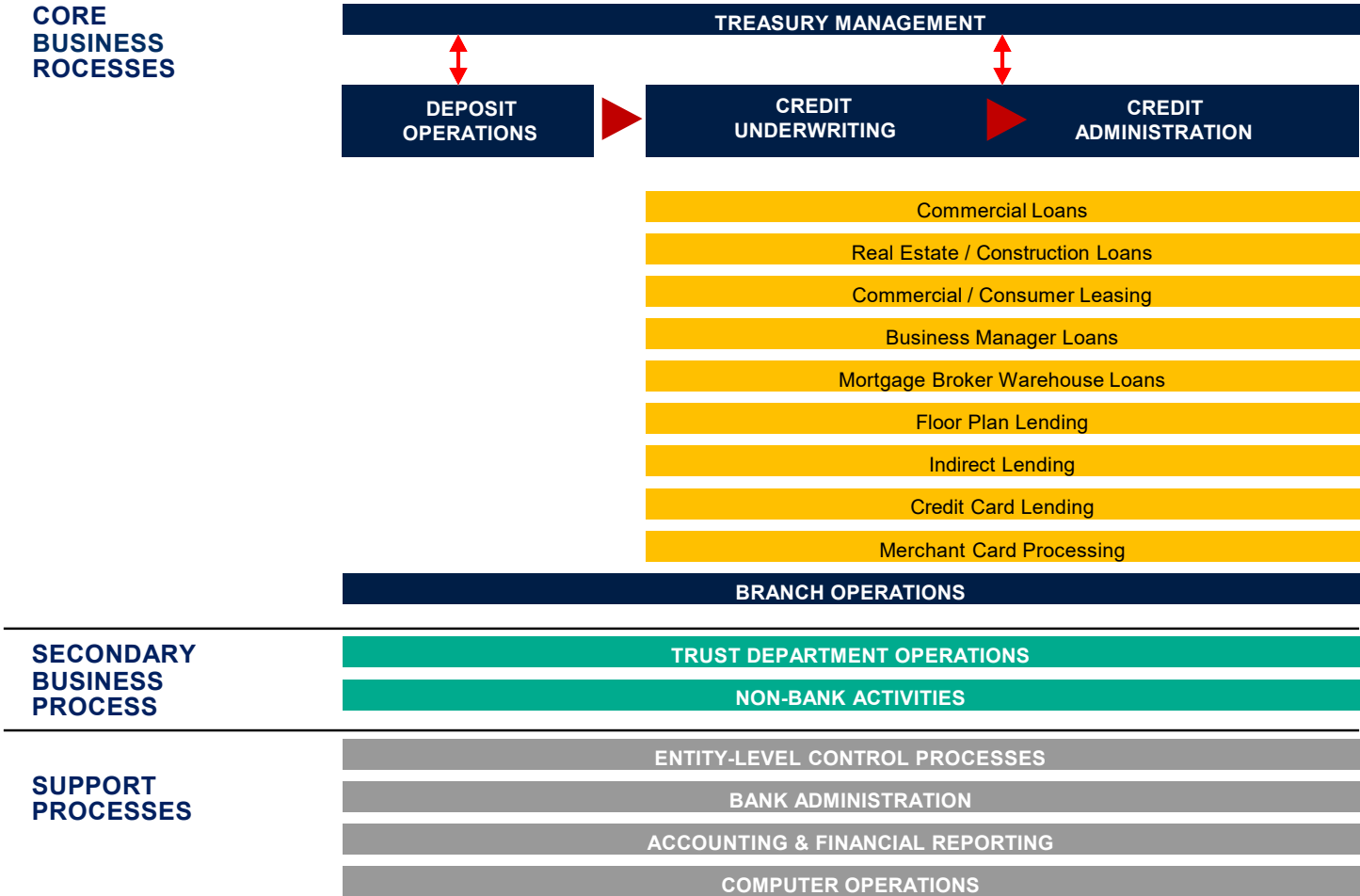
FDICIA/SOX Framework



Mapping Financial Statements to Key Financial Processes



Banking Industry Process “Universe”



Sample Mapping Document

Basic Financial Statement	ABC Bancorp, Inc. Amount From Internal Consolidation 06.30.03	Analysis		Degree of Estimation - (H=High, M=Moderate, L=Low)	Significant? Yes or No	Functional Areas														
		% of Assets	% of Equity			Lending Operations	Secondary Marketing	Treasury Management	Accounting & Financial Reporting	Deposit Operations	Branch Operations	Bank Administration	Trust	Information Technology	Regulatory Compliance					
Balance Sheet:																				
Cash	\$ 71,737,585	3%	31%	L	NO	X	X	X	X	X	X	X					X	X		
Interest-bearing cash deposits	11,387,045	0%	5%	L	YES			X	X									X		
Intercompany federal funds sold	-	0%	0%	L	NO			X	X									X		
Investment securities, AFS	884,450,535	35%	384%	M	YES			X	X									X		
FHLB stock	39,431,100	2%	17%	M	NO			X	X									X		
Federal Reserve Bank stock	5,250,350	0%	2%	M	YES			X	X									X		
Mortgage loans	290,225,972	12%	126%	L	YES	X			X		X						X	X		
Warehoused loans	48,830,746	2%	21%	L	YES	X	X		X		X						X	X		
Commercial loans	780,320,628	31%	339%	L	YES	X			X		X						X	X		
Consumer loans	285,410,580	11%	124%	L	YES	X			X		X						X	X		
Allowance for loan losses	(22,354,250)	-1%	-10%	H	YES	X			X								X	X		
Bank premises and equipment, net	48,657,893	2%	21%	M	YES				X				X				X			
Other real estate, net	682,405	0%	0%	M	NO	X			X								X			
Interest receivable	13,213,034	1%	6%	L	YES	X			X								X			
Core deposit intangible	6,192,973	0%	3%	H	YES				X								X			
Goodwill	33,189,234	1%	14%	H	YES				X								X			
Investment in subsidiaries	2	0%	0%	L	NO				X								X			
Deferred income taxes	-	0%	0%	M	NO				X								X			
Other assets	14,735,355	1%	6%	L	YES				X			X					X			
Total Assets	\$ 2,511,361,187	100%							X			X					X			

Sample Mapping Document

Basic Financial Statement	ABC Bancorp, Inc. Amount From Internal Consolidation 06.30.03	Analysis		Degree of Estimation - (H=High, M=Moderate, L=Low)	Significant? Yes or No	Affiliate 1		Affiliate 2		Affiliate 3	
		% of Assets	% of Equity			% Analysis	% Analysis	% Analysis	% Analysis		
Balance Sheet:											
Cash	\$ 71,737,585	3%	31%	L	NO	\$ 43,043	0%	\$ 18,526,154	26%	\$ 6,585,089	9%
Interest-bearing cash deposits	11,387,045	0%	5%	L	YES	-	0%	2,574,718	23%	1,039,630	9%
Intercompany federal funds sold	-	0%	0%	L	NO	-	NA	8,300,000	NA	-	NA
Investment securities, AFS	884,450,535	35%	384%	M	YES	-	0%	149,532,679	17%	55,529,459	6%
FHLB stock	39,431,100	2%	17%	M	NO	-	0%	7,048,400	18%	3,521,100	9%
Federal Reserve Bank stock	5,250,350	0%	2%	M	YES	-	0%	1,530,000	29%	215,650	4%
Mortgage loans	290,225,972	12%	126%	L	YES	-	0%	73,505,575	25%	12,529,884	4%
Warehoused loans	48,830,746	2%	21%	L	YES	-	0%	7,752,024	16%	506,030	1%
Commercial loans	780,320,628	31%	339%	L	YES	-	0%	192,585,977	25%	34,021,841	4%
Consumer loans	285,410,580	11%	124%	L	YES	-	0%	75,027,715	26%	26,296,184	9%
Allowance for loan losses	(22,354,250)	-1%	-10%	H	YES	-	0%	(4,282,887)	19%	(1,145,686)	5%
Bank premises and equipment, net	48,657,893	2%	21%	M	YES	-	0%	9,127,597	19%	1,769,381	4%
Other real estate, net	682,405	0%	0%	M	NO	-	0%	234,479	34%	-	0%
Interest receivable	13,213,034	1%	6%	L	YES	-	0%	2,622,686	20%	722,686	5%
Core deposit intangible	6,192,973	0%	3%	H	YES	-	0%	1,640,978	26%	-	0%
Goodwill	33,189,234	1%	14%	H	YES	-	0%	4,083,811	12%	260,048	1%
Investment in subsidiaries	2	0%	0%	L	NO	-	0%	-	0%	-	0%
Deferred income taxes	-	0%	0%	M	NO	-	NA	-	NA	-	NA
Other assets	14,735,355	1%	6%	L	YES	31,802	0%	1,839,938	12%	63,497	0%
Total Assets	\$ 2,511,361,187	100%				\$ 74,845	0%	\$ 551,649,844	22%	\$ 141,914,793	6%

Business Processes and Risk Owners

Business Processes	Risk Owner
Accounting and Financial Reporting	CFO
Allowance for Loan and Lease Losses (ALLL)	SVP
Deposit Operations	SVP
Electronic Banking (Wires/ACH)	Cashier
Entity Level	CFO
Information Technology	CIO
Lending – Commercial and Consumer	SVP
Mortgage Banking	SVP Mortgage Lending
Secondary Marketing	VP Mortgage Servicing
Payroll	HR Director
Retail Branches	Regional Ops Manager
Treasury Management	Cashier

Phase II: Project Planning



Objective

The objective of this phase is to establish a model for the form, level of documentation and testing that will meet all stakeholders needs. We will meet with the process owners to review the requirement, our methodology and overall project plan.



Assumptions

- Crowe will work with management to complete the tasks listed below but key stakeholders and members of management will need to review and approved the decisions.
- The Bank will assist with scheduling required meetings with key stakeholders.



Tasks

- Key Activities
 - Select documentation formats
 - Document control processes, identify key controls and design control testing plan
 - Reassess project plan assumptions redefine budgets



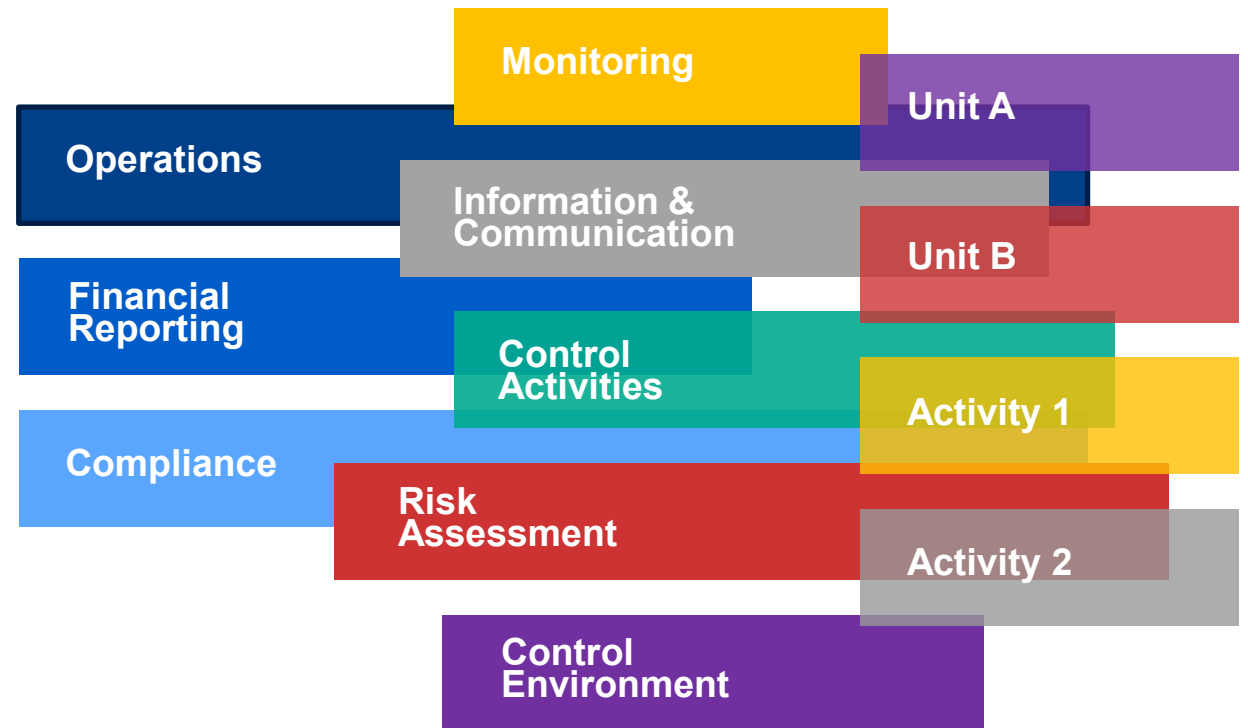
Deliverables

Conduct assessment:

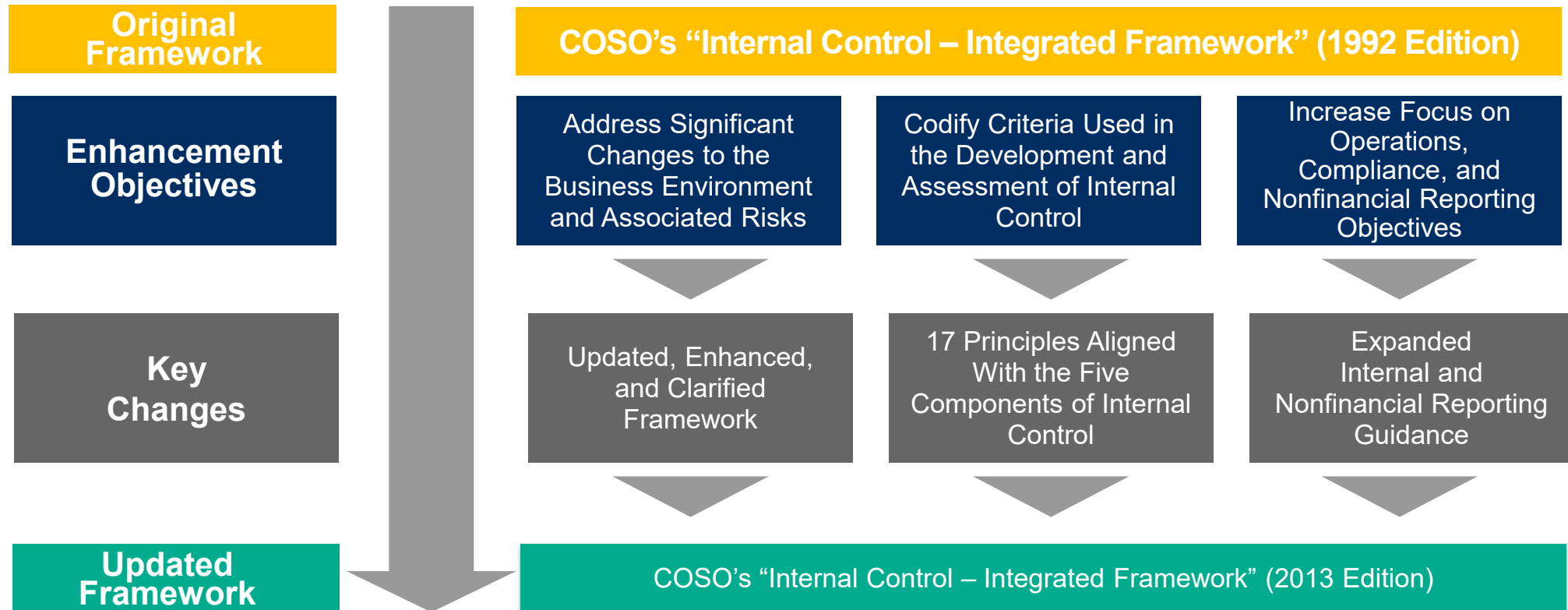
- Updated project plan
- Agreed upon documentation format
- Portal to provide our testing and documentation to key stakeholders and members of management

Integrated Framework: Overview

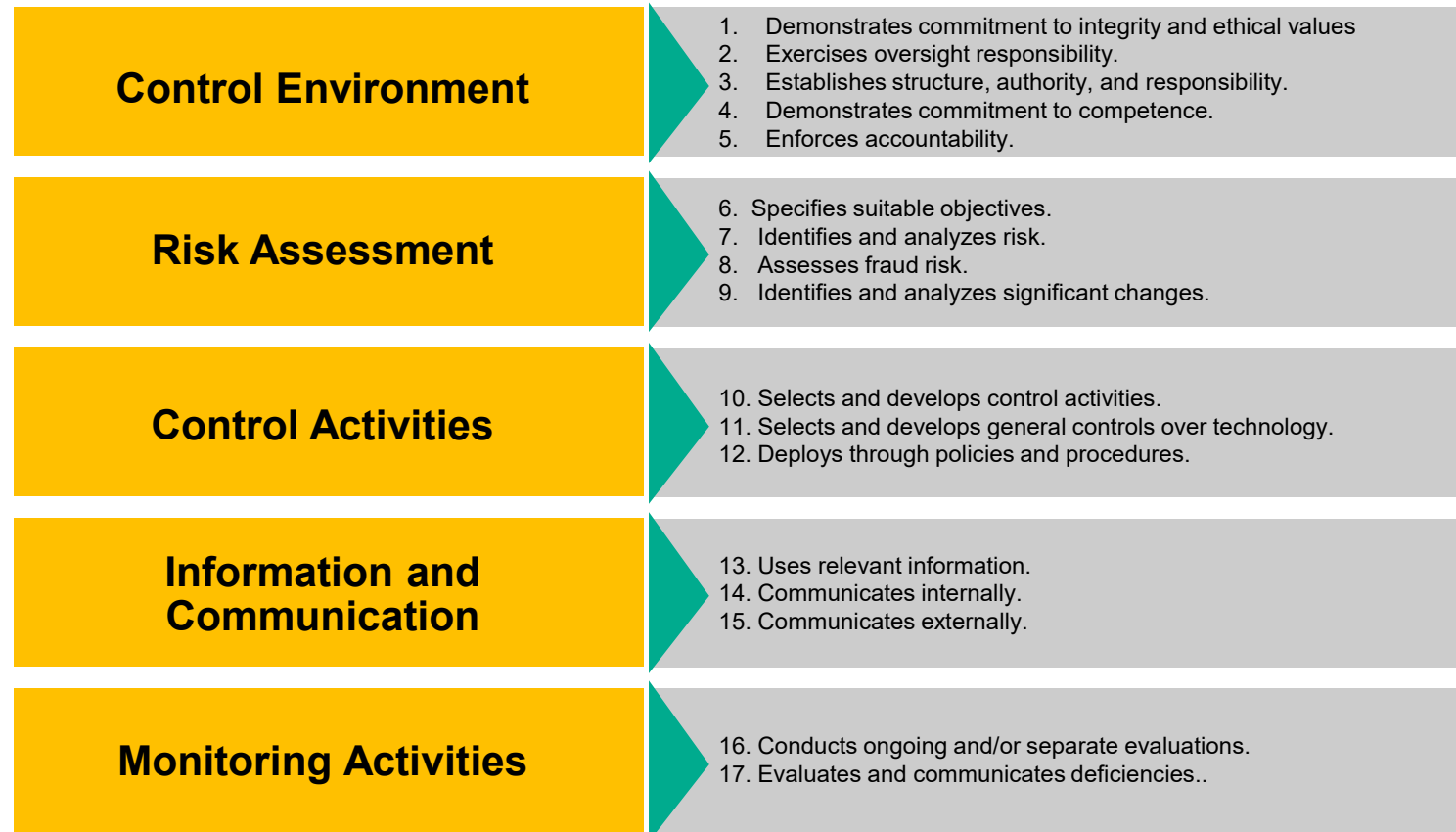
- First published in 1992; updated in 2013
- Gained wide acceptance following the financial control failures in the early 2000s and initial SOX years
- Most widely used framework for evaluating controls in the U.S.
- Widely used around the world
- Most companies publicly disclose if they are following the Framework



Integrated Framework: Project Objectives



COSO's Codification of Framework Principles



Sample Mapping Document

ABC Bancorp, Inc.	Significant (S) or Non Significant (N) Financial Statement/Disclosure Item	Centralized (C), Decentralized (D), Decentralized with Common Processes (P)	Application System(s) Interfacing with Named Business Process	Fin State Assert(s)	Parent	Affiliate 1	Affiliate 2	Affiliate 3	Affiliate 4	Affiliate 5	Affiliate 6	Affiliate 7
Key Business Processes												
GENERAL ENTITY LEVEL CONTROLS												
CONTROL ENVIRONMENT												
Board of Directors & Audit Committee	S	C / D	None	-	X	X	X	X	X	X	X	X
Integrity & Ethical Values	S	C / D	None	P	X	X	X	X	X	X	X	X
Human Resource Policies	S	C	None	-	X							
Organizational Structure	S	C / D	None	-	X	X	X	X	X	X	X	X
Management Operating Style	S	C / D	None	-	X	X	X	X	X	X	X	X
Transparency & Disclosure	S	C	None	P	X							
Legal & Regulatory	S	C	None	P	X							
Risk Management	S	C	None	-	X							
RISK ASSESSMENT												
Strategic Planning	S	C	None	-	X							
Enterprise Wide Risk Assessment	S	C	None	-	X							
CORPORATE POLICIES AND PROCEDURES												
Corporate Policies and Procedures	S	C / D	None	-		X	X	X	X	X	X	X
Information Systems	S	C	None	-	X							
MONITORING												
Budgeting & Analysis	S	P	None	-		X	X	X	X	X	X	X
Internal Audit Activities	S	P	None	-		X	X	X	X	X	X	X
CONTROL ACTIVITIES												
LENDING OPERATIONS												
Commerical Loans: Credit Policy and Underwriting	S	D	JH Silverlake	E, R, C		X	X			X	X	X
Consumer Loans: Credit Policy and Underwriting	S	D	JH Silverlake	E, R, C		X	X	X		X		
Real Estate Loans: Credit Policy and Underwriting	S	D	JH Silverlake	E, R, C		X			X		X	X

Phase III: Project Planning



Objective

The objective of this phase is to document and assess the overall control environment. Entity-level controls are pervasive and like general controls over information technology, are integral part of the company's overall control structure. We will utilize the agree upon documentation format to complete this phase.



Assumptions

- The Bank will assist with scheduling required meetings with key stakeholders.
- Items requested by Crowe will be provided in a timely manner.
- .



Tasks

- Key Activities
 - Walkthrough and review key processes and areas
 - Document key processes and areas
- Gap analysis of controls



Deliverables

Conduct assessment:

- Updated project plan
- Documentation of key processes and areas
- Gap analysis between existing and needed internal controls over financial reporting

Controls Documentation

1. Assessment of Existing Internal Controls Documentation for Significant Processes/Activities
2. Identification of documentation gaps or deficiencies
3. Determination of documentation format
 - Process maps for complex processes
 - Control matrices
 - Narratives
4. Walk through and documentation of controls with line management
5. Use of Subject Matter Experts to Assist in Documentation (IT, Trust, etc.)
6. Identification of control weaknesses
7. Remediation implementation process

Controls – Key vs. Supporting

- A key control is a control that, if it fails, means there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis. In other words, a key control is one that is required to provide reasonable assurance that material errors will be prevented or timely detected. Distinguish a process from a control. Remember that it is the process activities that may introduce errors in the financial statements. Controls are established to prevent or detect those errors.
- A supporting or mitigating control are those controls that help support the process but would not on their own detect a material error in the financial statements.
- If the scope and quality of management's identification, assessment, and testing of key controls is sufficient to address all major risks to the integrity of the financial statements and no material weaknesses are identified, then management will normally be able to assess the system of ICFR as effective. However, the presence of a single material weakness precludes management from making such an assessment. This is appropriate, as a material weakness by definition indicates that the system of internal control does not provide reasonable assurance regarding the reliability of the financial statements.

Management Review Controls (MRCs)

Examples of MRCs:

- Any review of analyses involving an estimate or judgment
- Reviews of financial results for components of a group
- Comparisons of budget to actual; and
- Review of impairment analyses.

Effective MRCs:

- Clear Accountability for Performance
- Appropriate Precision
- Performance based on a complete and accurate set of facts
- Performers with adequate knowledge and experience
- Clear Process for Performance

Sample Detailed Process and Documentation Hierarchy

1. Financial Statement Accounts – Commercial Loans
2. Key Process Areas –
 - Credit Underwriting
 - Credit Administration
3. Processes – Credit Administration
 - Disbursement authorization & funding
 - Collateral valuation, control, & security
 - Loan payment processing/application of principal & interest
 - Loan system input & file maintenance changes
 - Loan accounting & system reconciliation
 - Loan income recognition (interest & fees)
 - Collections, delinquencies, reserve for loan losses, charge-off's and recoveries
 - Other real estate owned (OREO) and repossessed assets
4. Control Activities/Techniques - Disbursement authorization & funding
 - Policies and procedures over loan documentation, approvals, and disbursement of loan proceeds have been established
 - Appropriate individuals are assigned the authority for approving loan disbursements
 - Loan documentation is reviewed prior to disbursement of proceeds
 - Documentation deficiencies are corrected prior to the disbursement of loan proceeds
 - Loan disbursement checks or internal credits are prepared from original loan documents and signed by an individual other than the preparer, within their authorization limit
 - Funding exceptions are monitored and reported to an appropriate level of management
 - Tickler systems have been established to monitor stale borrower credit information

Sample Control Documentation

BankName ICOFR Documentation of Controls	
Business Process:	<u>Goodwill and Intangible Assets</u>
Process Documentation:	
Goodwill and Intangible Assets Reconciliations	
Goodwill and Intangible Assets related subsidiary ledgers are maintained and reconciled quarterly from the subsidiary ledger to the general ledger control accounts. Reconcilements are prepared and then reviewed by supervisory personnel according to the procedures in Bank Policy. In the event the individual responsible for preparation of the reconciliation is not independent from the function, the reconciliation will be subject to an additional level of detail of review including:	
- Tracing and testing a sample of reconciling items (sample size to be based upon volume)	
- Re-footing the reconciliation	
Evidence of preparation and review is documented via physical or electronic signature and date on a formal reconciliation cover sheet. Reconciling items are identified, described, and then generally cleared within 90 days. Key Control #1.	
Goodwill and Intangible Assets Impairment Review	
On an annual basis, a member of the Accounting Department or CFO performs an Impairment Analysis to determine if goodwill or intangible assets are impaired. If a material event occurs in an interim period, The CFO will perform an analysis at that time. If an Impairment has occurred, an entry will be prepared to write-down the carrying value of goodwill or intangible assets. The Member of the Accounting Department or CFO (whomever does not perform the impairment analysis) reviews and approves the analysis. Evidence of the review and approval is retained. Key Control #2.	
<u>Management Review</u>	
Reviewed by:	_____
Reviewer's Title:	_____
Date Reviewed:	_____


Sample Controls Documentation Matrix

ABC CORPORATION
SECTION 404 INTERNAL CONTROL AGREEMENT
KEY BUSINESS PROCESS = COMMERCIAL LENDING (DRAFT)

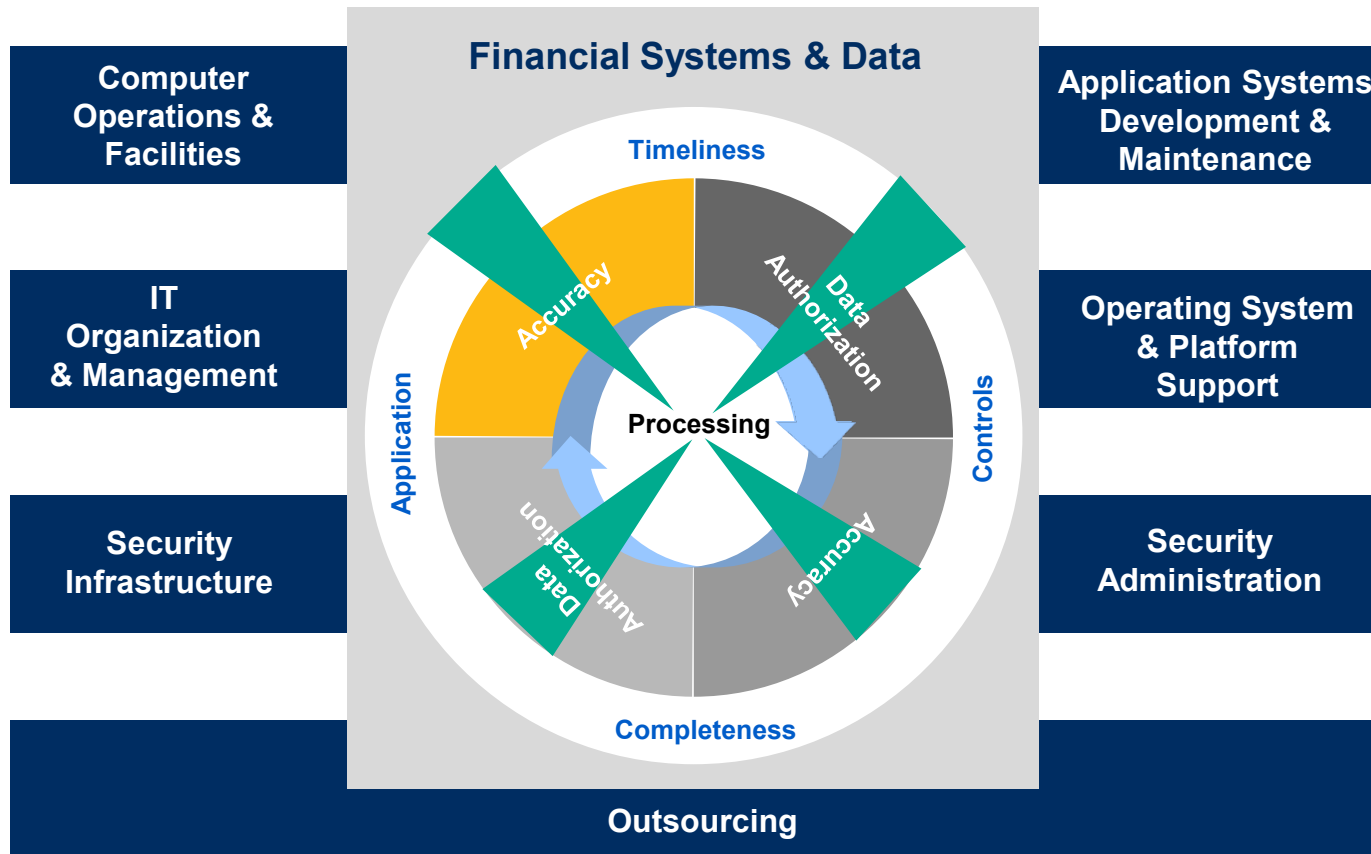
CONTROL OBJECTIVE RISK FACTORS <u>Commercial Lending</u>	FS ASSERTIONS	TYPICAL CONTROL TECHNIQUES	DOCUMENTATION OF CONTROL PROCESSES	TYPE	KEY	TESTING PROCEDURES	FREQ.	RESP.
Authorization Loans are originated in a manner that creates poor quality loans, loans to ___ borrowers, or loans are not properly priced for the corresponding level of associated risk. This could result in an inability to collect principal and/or reduced interest income.	E, V, R	1. The Bank has formerly established and documented a loan policy. The loan policy is periodically presented to the Board and approved. The approval is documented in the Board minutes. Management has also documented procedures for significant loan functions.		P				
<u>Authorization</u> See 1. Above	E, V, R	2. Loan policy establishes underwriting criteria and guidelines, including loan authority. The policy authorizes any two loan officers with the appropriate loan authority to approve various types of loans (i.e., participations, lines of credit, etc.) Individual loan authorities are formally documented and approved by the Board of Directors		P				
<u>Evaluation of Balances</u> Loan quality and borrower's financial condition are not properly or timely monitored, or inaccurate monitoring information is obtained, resulting in reduced ability to collect interest or principal.	E, V, R	3. All loans greater than \$250,000 are required to receive a formal review by the Loan Officer at least annually. All loans greater than \$1,000,000 receive an annual review that includes analysis from the Credit Administration department. This review is formally documented in the file.		M	X	Judgmentally select a sample of 8 loans greater than \$1,000,000 that have been in the portfolio for more than 1 year. Obtain the corresponding credit file and verify that an annual review of the loan has been completed in accordance with established requirements. Also, determine that the review is adequately documented in the file and performed by someone independent of approval authority. Workpaper ___ Performed by ___ Request items: All ___ of loans greater than \$1MM	Qtrly	Jennifer D.

Financial Statement Assertions: E = Existence Occurrence; C = Completeness; V = Valuation; R = Rights & Obligations; P&D = Presentation & Disclosure

Control Types: M = Monitoring Control; P = Procedure Process Control; DC = Defective Control; PC = Preventive Control

 = Anti-Fraud Control at the Process Level

Sample IT General & Application Controls



Phase IV: Conduct Testing



Objective

Based upon the key controls identified in the earlier phases we execute testing for all key controls identified and confirmed by management. Effectiveness of the controls will be accumulated and reviewed with management to determine if any remediation and additional testing is needed.



Assumptions

- Management will review and confirm the accuracy of the key controls identified prior to testing by Crowe.
- Management will provide the items requested by Crowe in a timely manner to complete the control testing.
- Management is keeping their external auditor updated on the status of the project.



Tasks

- Key Activities
 - Complete key control testing
 - Identify best practice recommendations
 - Provide summary of testing results



Deliverables

Conduct testing:

- Updated project plan
- Document showing testing results and effectiveness of controls
- Best practice recommendations memo



Identification and Testing of Key Controls

1. Management identification of Key Controls over Financial Reporting
 - Key controls are tested annually
 - Non-key controls can be rotated
2. Testing plan should define nature, timing and extent of testing and who should perform testing
3. Testing should tie into existing IA testing program although some testing will need to be done by management
4. Need to have external auditor buy-in to test plan

Phase V: Report Results



Objective

The objective of this phase is to summarize the results of the documentation and testing of the key controls to enable management to prepare their annual assessment of internal controls over financial reporting.



Assumptions

- Management will provide the final report and their annual assessment to their external auditors.



Tasks

- Key Activities
 - Summarize key controls
Crowe leads.
 - Management prepare annual assessment
Crowe Assists.

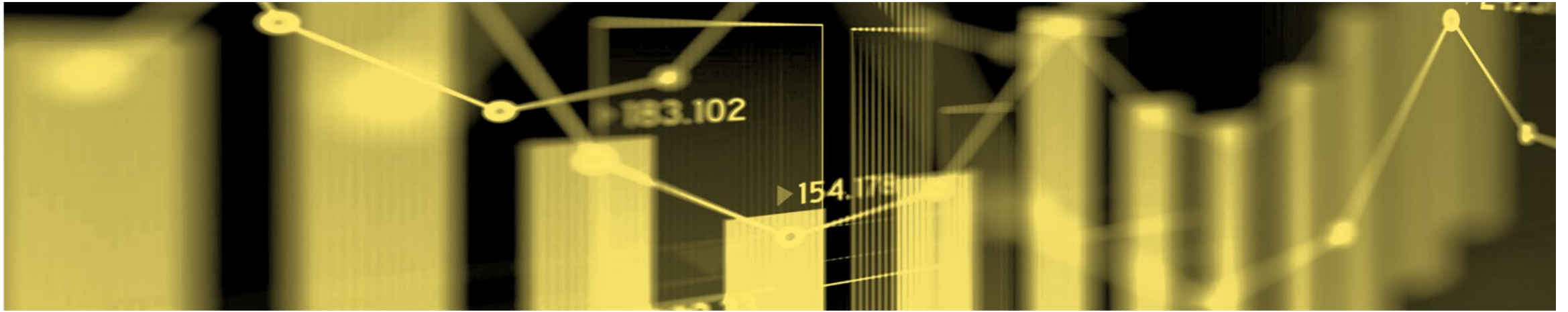


Deliverables

- Final report summarizing the design and operating effectiveness of the key controls identified and testing.

Management's Assessment

- The methods of conducting evaluations will, and should, **vary from bank to bank**
- The assessment must be based on procedures sufficient both to evaluate its **design and operating effectiveness**
- The **nature of a bank's testing** activities will largely depend on the **circumstances** of the bank and the **significance** of the control
- **Inquiry** alone generally **will not provide** an adequate basis for management's assessment



Managing the Data

Philosophy About Technology Tools

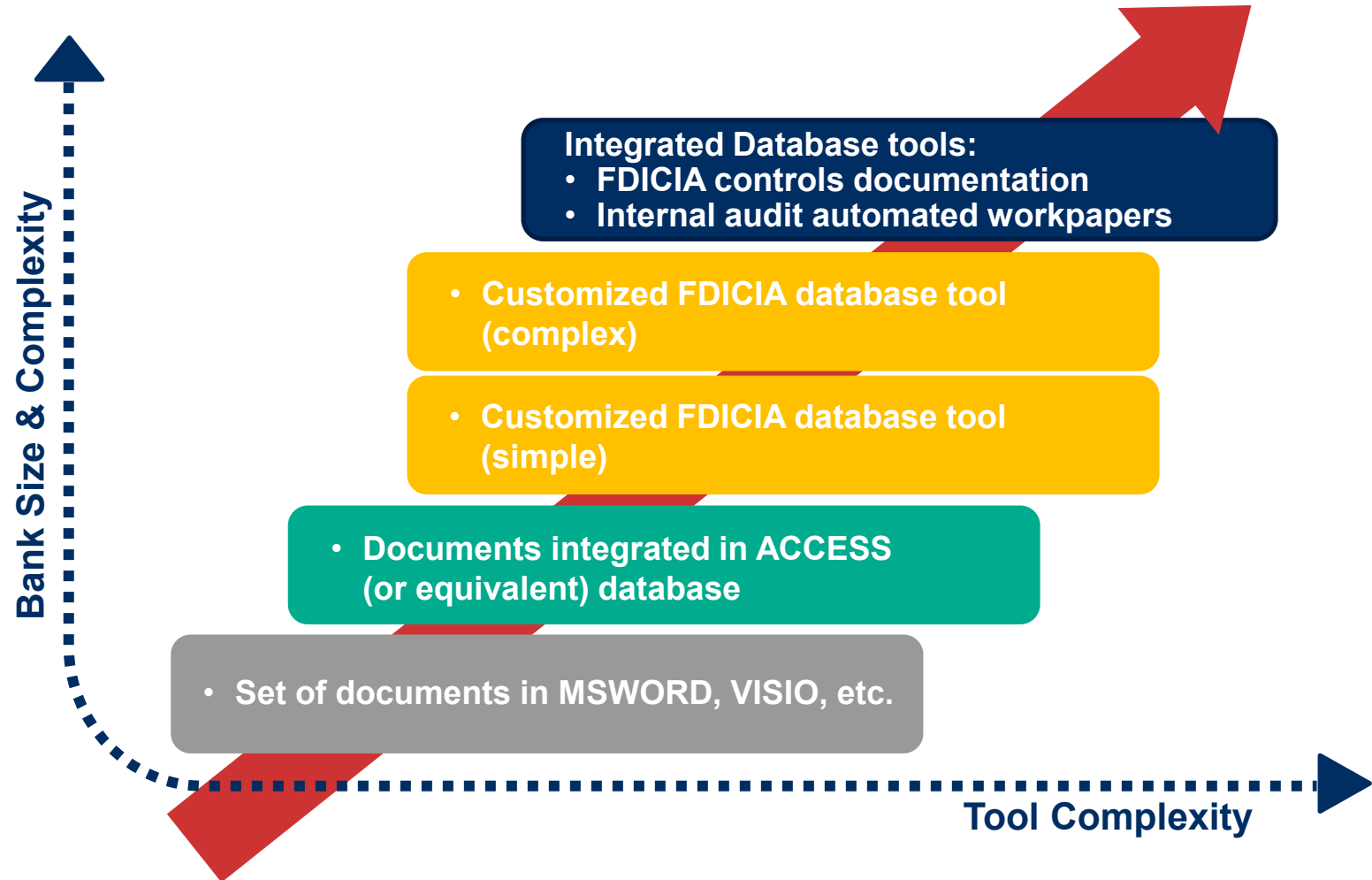
- The FDICIA process should drive technology, **not** the other way around
- There is no “silver bullet” tool for FDICIA
- Tools are more important in managing documentation & testing over time than in establishing initial documentation



Match Tool Options to Needs

Based On Number Of:

- Banking processes
- Systems
- Non-bank subs./activities
- Locations





Conclusions and Questions



Conclusions

- View FDICIA/SOX compliance as an opportunity to improve controls and Corporate Governance
- Make sure you have a structured approach that makes sense for your institution
- Involve all of the right people
- Get started
- Don't let the technology tail wag the dog



Polling Question #3

Following this session, do you feel more comfortable with the topic of FDICIA/SOx compliance?

- A. Yes
- B. Somewhat
- C. Not really



Exercise

For the area assigned to your group (Loans, Deposits, General Accounting, Investments, Information Technology):

- Identify at least three “Key controls over financial reporting”.
- For each Key Control identified, create one or more “tests of operating effectiveness” that would illustrate that the Key Control was functioning.



PPP Loan Forgiveness

Presented by Maddie Stupinski



Polling Question #1

How comfortable are you when it comes to the topic of PPP Loan Forgiveness?

- A. Very comfortable
- B. Fairly comfortable
- C. Only slightly comfortable
- D. What PPP?

PPP Forgiveness Program Considerations and Evolution

- The PPP Forgiveness Program rules and guidance have changed over time
- Changes indicate intent of SBA to truly help borrowers
- Potential for additional guidance and changes in the future



What are PPP Loans?

The CARES Act was signed on March 27, 2020 with the aim to support small businesses throughout the pandemic. The CARES Act included the Payment Protection Program (PPP) which is a \$953-billion business loan program intended to provide small businesses with funds to support the following business purposes:

- Payroll
- Mortgage Interest
- Rent
- Utilities



If the business's spending meets specific stipulations set by the SBA, up to their entire loan may be forgiven. The specific stipulations are as follows:

- All funds are used within the covered period (8- or 24-weeks from the date of disbursement)
- 60% of the loan must be used on payroll
- Maintain staffing level (FTE levels cannot be reduced unless specific safe harbors have been met)
- Maintain at least 75% of the total salary level

Note that the above stipulations are subject to change due to SBA Guidance updates.

Program History

SBA Loan Program

Unsecured loans to pay certain eligible costs, which can be forgiven

First Round

\$349B - April 2020 – First Come, First Served – Ran out of money

Second Round

\$349B - June 2020 to August 2020 – Did not run out of money

Third Round

\$285B - January 19 to March 31, 2021 – Just had enough money

Bank/Borrower Experience

First two rounds were hectic and challenging for banks and borrowers

PPP Loan Terms – A Really Good Deal

- Loans up to \$10,000,000 for First Draw, \$2,000,000 for Second Draw
- Interest Rate of 1%
- Unsecured
- No personal guarantees
- 100% SBA guarantee to lender
- Loan funds used to pay eligible costs during a Covered Period of 8 to 24 weeks will be **forgiven** by the SBA and repaid to the lender, along with interest accrued
- Repayment over 5 years of any remaining balance not forgiven

PPP Loan Programs

1

New “First Draw” PPP Loans

Businesses which did not receive a PPP loan in 2020, may be eligible for a First Draw PPP loan

2

“Second Draw” PPP Loans

Some businesses will be eligible for a Second Draw PPP loan, if certain requirements are met

Polling Question #2

Did you implement a technology to help support your PPP process?

- A. Yes, for origination.
- B. Yes, for forgiveness.
- C. Yes, for both origination and forgiveness.
- D. No, we are processing these applications manually.

First Draw PPP Loans

Eligibility Requirements



Employ no more than 500 employees, unless Borrower meets SBA size standard for their industry

Were in operation on February 15, 2020

Not permanently closed

Borrower makes various certifications on application

Did not receive a PPP loan in 2020

Loan Amount Calculation



In general, Borrowers may receive a loan amount of *2.5 months* of average monthly eligible payroll costs from 2019 or the 12 months prior to the loan

Seasonal employers may use a 12-week period for determining average monthly eligible payroll costs

Excluding non-U.S. residents and pay over annualized \$100,000

Limited to \$10,000,000 (or \$20 million for a corporate group)

Eligible Entities



- Sole Proprietors
- Business Partnerships
- Business Corporations
- Non-Profits
- Religious organizations
- 501(c)(6)
- Housing cooperative
- Tribal concerns
- News organizations

- There are several ineligible types
 - Illegal Activities
 - Publicly traded
 - Household
 - Felon as an owner
 - Defaulted on past SBA loan

Eligible Payroll Costs for calculating loan amount

- Employee Compensation
 - U.S. Residents only (whether a citizen or not)
 - Compensation includes salary, wages, and other cash compensation categories (see below)
 - Compensation to any individual above a \$100,000 annualized rate must be excluded
- Employee Benefits Costs paid by employer (not the employee portion)
- Employee Retirement Contributions paid by employer (not the employee portion)
- State and local payroll-based taxes
- Sole Proprietors (or Independent Contractors) income

With respect to “purpose of the loan,” payroll costs consist of compensation to employees (whose principal place of residence is the United States) in the form of salary, wages, commissions, or similar compensation; cash tips or the equivalent (based on employer records of past tips or, in the absence of such records, a reasonable, good-faith employer estimate of such tips); payment for vacation, parental, family, medical, or sick leave (except those paid leave amounts for which a credit is allowed under FFCRA Sections 7001 and 7003); allowance for separation or dismissal; payment for the provision of employee benefits (including insurance premiums) consisting of group health care coverage, group life, disability, vision, or dental insurance, and retirement benefits; payment of state and local taxes assessed on compensation of employees; and, for an independent contractor or sole proprietor, wage, commissions, income, or net earnings from self-employment or similar compensation.

First Draw PPP Loan Application Documents

Eligibility

- **Employee Counts:**
 - Payroll Reports, or
 - Payroll Tax Filings
- **Documentation of Operation at 2/15/2020**
 - Payroll, or bank accounts

Entity

- **Documentation of Existence**
 - Proof of entity type
 - Schedule of Owners (names, percentages)

Loan Amount

- **2019 Calendar Year Payroll Cost Report** listing all employees and total wages
 - Applying required annualized \$100,000 caps on eligible compensation
 - Only U.S. residents
 - Third party payroll processors may have special PPP reports
- **Evidence of other payroll costs** during 2019
 - Employer contributions for employee group health life, disability, vision and dental insurance
 - Employer contributions to employee retirement plans
- Note: 2020 payroll costs are allowable as an option

Depending on loan size and business complexity, other documents may be required.

Second Draw PPP Loans

Eligibility Requirements



Employ no more than 300 employees

Demonstrate at least a 25% reduction in gross receipts for either the first, second, third or fourth quarter of 2020, relative to the same quarter in 2019.

Have used or will use the first PPP loan funds by time second loan is disbursed

Were in operation on 2/15/2020

Have not already received a Second Draw loan

Loan Amount Calculation



In general, same as original PPP loan

Industries assigned to NAICS code 72 (lodging and restaurants) may receive loans up to *3.5 months* of average monthly eligible payroll costs

Limited to \$2,000,000 (or \$4,000,000 for a corporate group)

Eligible Entities



Same as for First Draw PPP Loans,

Except additional Ineligible Entities

- Publicly traded
- China related
 - Organized in China
 - Significant China operations
 - China resident as board member
- Lobbying or think tank
- Permanently closed

Second Draw PPP Loan Application Documents

Eligibility

- **Documentation required to demonstrate the revenue reduction:**
 - Quarterly Income Statement for selected quarter in 2020
 - Quarterly Income Statement for 2019
 - Same quarter as selected in 2020
 - Note: full year may be used, and under \$150K can wait to provide until requesting forgiveness

Other Documents similar to First Draw

Entity

- **Same as First Draw Loan**

Loan Amount

- **2019 Calendar Year Payroll Cost Report** listing all employees and total wages
 - Applying required annualized \$100,000 caps on eligible compensation
 - Only U.S. residents
 - Third party payroll processors may have special PPP reports
- **Evidence of other payroll costs** during 2019
 - Employer contributions for employee group health life, disability, vision and dental insurance
 - Employer contributions to employee retirement plans
- Note: 2020 payroll costs and employee counts are allowable as an option

Depending on loan size and business complexity, other documents may be required.

PPP Structure

	CARES Act (March 27, 2020)	PPP Flexibility Act (June 5, 2020)	Consolidated Appropriations Act (Dec. 27, 2020)
Program period	Feb. 15 – June 30, 2020	Feb. 15 – Dec 31, 2020	Extended through March 31, 2021
Covered period of expenses	Up to 8 weeks	Up to 24 weeks	
Forgivable expenses	Payroll, employee benefits, mortgage interest, rent, and utilizes (max of 25% non-payroll costs)	Increases limitation on non-payroll costs from 25% to 40%	Expanding eligible expenses
Maturity	Capped at 10 years; Treasury capped at 2 years	Capped at 5 years minimum	
Payment deferral	6 months	Until SBA remits to lender any forgiven amounts; Or, for borrowers not applying for forgiveness, until 10 months after conclusion of covered period	

PPP Appropriations

Rollforward (\$B) as of Jan. 31, 2021			
CARES	PPP & Healthcare	Consolidated	
<ul style="list-style-type: none"> • HR 748 • Mar. 27, 2020 • \$349B funded 	<ul style="list-style-type: none"> • HR 266 • Apr. 24, 2020 • \$310B funded 	<ul style="list-style-type: none"> • HR 133 • Dec. 27, 2020 • \$284B funded 	\$349
<ul style="list-style-type: none"> • Expired Apr. 16, 2020 • Funds exhausted . 	<ul style="list-style-type: none"> • Expired Aug. 8, 2020 • End of program • \$134B remained 	<ul style="list-style-type: none"> • Expires Mar. 31, 2021 (or until exhausted) 	<ul style="list-style-type: none"> - 349 <u>0</u>
			+310
			- 176
			<u>134</u>
			+ 284
			<u>418</u>
			- 73
			<u>\$345</u>



Key changes: Consolidated Appropriations Act

DIVISION N—ADDITIONAL CORONAVIRUS RESPONSE AND RELIEF

TITLE III—CONTINUING THE PPP AND OTHER SMALL BUSINESS SUPPORT

- Section 323: Commitment Authority and Appropriations
 - Extends program to March 31, 2021, authorization level at \$806.5 billion
- Section 303: Emergency Rulemaking Authority
 - SBA established regulations no > 10 days after enactment
- Section 304: Additional eligible expenses
 - Operations, property damage, supplies costs and PPE

Key changes: Consolidated Appropriations Act

- Section 311: PPP second draw loans
 - < 300 employees; demonstrate reduction of gross receipts of 25% in Q1, Q2 or Q3
 - Maximum loan amount of \$2M
- Section 342: Prohibition of Eligibility for Publicly Traded Companies.
 - Excludes publicly traded companies, except for certain news organizations
- Section 307: Simplified application process for loans under \$150,000
 - Borrower shall receive forgiveness if a borrower signs and submits to the lender a certification that is not more than one page in length (created by SBA within 24 days)
 - Borrowers are required to retain relevant records related to employment (4 years) and other records (3 years). SBA may audit to ensure against fraud.

Key changes: Consolidated Appropriations Act

- Section 333: Repeal of Economic Injury Disaster Loan (EIDL) advance deduction
 - Repeals CARES section 1110(e)(6) which requires PPP borrowers to deduct the amount of their EIDL advance from their PPP forgiveness amount
- Section 340: Reimbursement for Processing
 - For loans < \$50,000, fees are lesser of 50% of loan principal or \$2,500 (the fee was 5%)
 - Agent fees clarified that not deducted from lender's processing fees if no agent contract in place with the lender
- TITLE II—ASSISTANCE TO INDIVIDUALS, FAMILIES, AND BUSINESSES
- Section 276: Clarification of Tax Treatment of Forgiveness of Covered Loans
 - No amount shall be included in the gross income; no deduction shall be denied

EIDL Program Updates

- Provides additional targeted funding for eligible entities located in low-income communities through the EIDL advance program of the CARES Act
 - Entities in low-income communities that received the EIDL advance under the CARES Act are eligible to receive the amount equal to the difference of what they received under the CARES Act and \$10,000
- Provides funding for eligible applicants that did not receive EIDL because original funding was exhausted before they could receive funds
- Emergency EIDL grants are extended through December 31, 2021
 - Time is extended for the SBA to approve and disburse the Emergency EIDL loans from 3 days to 21 days
- As mentioned previously, the new legislation provides that EIDL advances are not required to be deducted from PPP loan Forgiveness

Grants for Shuttered Venue Operators

- The new legislation authorized \$15 billion for the SBA to make grants available to eligible entities in the entertainment sector including:
 - Live venue operators or promoters
 - Theatrical producers
 - Live performing arts organization operators
 - Museums
 - Movie theatres and talent representatives
- Entities must show at least a 25% reduction in revenues
- Funds will be released in a phased approach with the hardest-hit entities receiving funds first
 - Grants will be given in the first 14 days to entities that have faced a 90% or greater revenue loss
 - A second 14-day period will be reserved for entities that faced 70% or greater revenue loss
 - After these two periods grants will be given to all other eligible entities
- Funds shall be used for eligible payroll, rent, utilities and personal protective equipment (PPE) costs
- Receiving this grant makes entities ineligible for a PPP loan

Tax Treatment

- Forgiveness amount is not taxable income
 - The COVIDTRA clarifies that the non-taxable treatment of PPP loan Forgiveness that was provided by the 2020 CARES Act also applies to certain other forgiven obligations
- Expenses used to support Forgiveness are now tax deductible
 - The COVIDTRA clarifies that taxpayers with PPP loans or other obligations are forgiven as described above, are allowed deductions for otherwise deductible expenses paid with the proceeds and that the tax basis and other attributes of the Borrower's assets won't be reduced as a result of the Forgiveness
- Waiver of information reporting for PPP loan Forgiveness
 - The COVIDTRA allows IRS to waive information reporting requirements for any amount excluded from income under the exclusion- from-income rule for Forgiveness of PPP loans or other specified obligations
- Borrowers with PPP loans may also qualify for the Employee Retention Tax Credit (ERTC) if PPP and ERTC do not cover the same payroll expenditures
- Borrowers may continue to defer payroll taxes until the PPP loan is forgiven
 - 50% of the payroll taxes must be paid by December 31, 2021
 - The remaining 50% must be paid by December 31, 2022

PPP Loan Forgiveness Applications

Paycheck Protection Program
Loan Forgiveness Application Form 3508 Revised January 19, 2021
OMB Control No.: 3245-0087
Expiration Date: 7/31/2021

PPP Loan Forgiveness Calculation Form

Business Legal Name ("Borrower")		DBA or Tradename, if applicable	
Business Address	NAICS Code	Business TIN (EIN, SSN)	Business Phone
Primary Contact		Primary Contact	E-mail Address

First Draw PPP Loan Second Draw PPP Loan (check one)

SBA PPP Loan Number: _____ Lender PPP Loan Number: _____

PPP Loan Amount: _____ PPP Loan Disbursement Date: _____

Employees at Time of Loan Application: _____ Employees at Time of Forgiveness Application: _____

Covered Period: _____ to _____

If Borrower (together with Affiliates, if Applicable) Received First Draw PPP Loans of \$2 Million or More or Second Draw PPP Loans of \$2 Million or More, check here:

Forgiveness Amount Calculation:

Payroll and Nonpayroll Costs

Line 1. Payroll Costs (enter the amount from PPP Schedule A, line 10): _____

Line 2. Business Mortgage Interest Payments: _____

Line 3. Business Rent or Lease Payments: _____

Line 4. Business Utility Payments: _____

Line 5. Covered Operations Expenditures: _____

Line 6. Covered Property Damage Costs: _____

Line 7. Covered Supplier Costs: _____

Line 8. Covered Worker Protection Expenditures: _____

Adjustments for Full-Time Equivalency (FTE) and Salary/Hourly Wage Reductions

Line 9. Total Salary/Hourly Wage Reduction (enter the amount from PPP Schedule A, line 3): _____

Line 10. Sum the amounts on lines 1 through 8, then subtract the amount entered in line 9

Line 11. FTE Reduction Quotient (enter the number from PPP Schedule A, line 13): _____

Potential Forgiveness Amounts

Line 12. Modified Total (multiply line 10 by line 11): _____

Line 13. PPP Loan Amount: _____

Line 14. Payroll Cost 60% Requirement (divide line 1 by 0.60): _____

Forgiveness Amount

Line 15. Forgiveness Amount (enter the smallest of lines 12, 13, and 14): _____

Paycheck Protection Program
PPP Loan Forgiveness Application Form 3508EZ Revised January 19, 2021
OMB Control No.: 3245-0087
Expiration Date: 7/31/2021

PPP Loan Forgiveness Calculation Form

Business Legal Name ("Borrower")		DBA or Tradename, if applicable	
Business Address	NAICS Code	Business TIN (EIN, SSN)	Business Phone
Primary Contact		Primary Contact	E-mail Address

First Draw PPP Loan Second Draw PPP Loan (check one)

SBA PPP Loan Number: _____ Lender PPP Loan Number: _____

PPP Loan Amount: _____ PPP Loan Disbursement Date: _____

Employees at Time of Loan Application: _____ Employees at Time of Forgiveness Application: _____

Covered Period: _____ to _____

If Borrower (together with Affiliates, if Applicable) Received First Draw PPP Loans of \$2 million or More or Second Draw PPP Loans of \$2 Million or More, check here:

Forgiveness Amount Calculation:

Payroll and Nonpayroll Costs

Line 1. Payroll Costs: _____

Line 2. Business Mortgage Interest Payments: _____

Line 3. Business Rent or Lease Payments: _____

Line 4. Business Utility Payments: _____

Line 5. Covered Operations Expenditures: _____

Line 6. Covered Property Damage Costs: _____

Line 7. Covered Supplier Costs: _____

Line 8. Covered Worker Protection Expenditures: _____

Potential Forgiveness Amounts

Line 9. Sum the amounts on lines 1 through 8: _____

Line 10. PPP Loan Amount: _____

Line 11. Payroll Cost 60% Requirement (divide Line 1 by 0.60): _____

Forgiveness Amount

Line 12. Forgiveness Amount (enter the smallest of Lines 9, 10, and 11): _____

Paycheck Protection Program
PPP Loan Forgiveness Application Form 3508S
OMB Control No.: 3245-0087
Expiration Date: 10/31/2020

PPP Loan Forgiveness Calculation Form

A BORROWER MAY USE THIS FORM ONLY IF THE BORROWER RECEIVED A PPP LOAN OF \$50,000 OR LESS. A Borrower that, together with its affiliates, received PPP loans totaling \$2 million or greater cannot use this form.

Business Legal Name ("Borrower")		DBA or Tradename, if applicable	
Business Address	Business TIN (EIN, SSN)	Business Phone	
Primary Contact		Primary Contact	E-mail Address

SBA PPP Loan Number: _____ Lender PPP Loan Number: _____

PPP Loan Amount: _____ PPP Loan Disbursement Date: _____

Employees at Time of Loan Application: _____ Employees at Time of Forgiveness Application: _____

EIDL Advance Amount: _____ EIDL Application Number: _____

Forgiveness Amount: _____

By Signing Below, You Make the Following Representations and Certifications on Behalf of the Borrower:

The Authorized Representative of the Borrower certifies to all of the below by initialing next to each one:

The dollar amount for which forgiveness is requested does not exceed the principal amount of the PPP loan and:

- was used to pay costs that are eligible for forgiveness (payroll costs to retain employees; business mortgage interest payments; business rent or lease payments; or business utility payments);
- includes payroll costs equal to at least 60% of the forgiveness amount;
- if a 24-week Covered Period applies, does not exceed 2.5 months' worth of 2019 compensation for any owner-employee or self-employed individual (general partner, capped at \$20,833 per individual); and
- if the Borrower has elected the 8-week Covered Period, does not exceed 8 weeks' worth of 2019 compensation for any owner-employee or self-employed individual (general partner, capped at \$20,833 per individual).

The borrower has not used any of the funds for the purpose of paying any federal, state, or local tax liability or for the purpose of unwise recovery of loan amounts and/or civil or criminal fraud charges.

The Borrower has accurately verified the payments for the eligible payroll and nonpayroll costs for which the Borrower is requesting forgiveness, and has accurately calculated the forgiveness amount requested.

I have submitted to the Lender the required documentation verifying payroll costs, the existence of obligations and service (as applicable) prior to February 15, 2020, and eligible business mortgage interest payments, business rent or lease payments, and business utility payments.

The information provided in this application and the information provided in all supporting documents and forms is true and correct in all material respects. I understand that knowingly making a false statement to obtain forgiveness of an SBA-guaranteed loan is punishable under the law, including 18 USC 1001 and 3571 by imprisonment of not more than five years and/or a fine of up to \$250,000; under 15 USC 645 by imprisonment of not more than two years and/or a fine of not more than \$5,000; and, if submitted to a Federally insured institution, under 18 USC 1014 by imprisonment of not more than thirty years and/or a fine of not more than \$1,000,000.

The tax documents I have submitted to the Lender are consistent with those the Borrower has submitted/will submit to the IRS and/or state tax or workforce agency. I also understand, acknowledge, and agree that the Lender can share the tax information with SBA's authorized representatives, including authorized representatives of the SBA Office of Inspector General, for the purpose of ensuring compliance with PPP requirements and all SBA reviews.

I understand, acknowledge, and agree that SBA may request additional information for the purposes of evaluating the Borrower's eligibility for the PPP loan and for loan forgiveness, and that the Borrower's failure to provide information requested by SBA may result in a determination that the Borrower was ineligible for the PPP loan or a denial of the Borrower's loan forgiveness application.

The Borrower's eligibility for loan forgiveness will be evaluated in accordance with the PPP regulations and guidance issued by SBA through the date of this application. SBA may direct a lender to disapprove the Borrower's loan forgiveness application if SBA determines that the Borrower was ineligible for the PPP loan.

Signature of Authorized Representative of Borrower _____ Date _____

Print Name _____ Title _____

Rules for Calculating Amount of Forgiveness are the Same for All forms

3508 Standard Form

- Loans over \$150,000
- FTE changes occurred during the Covered Period (*beyond allowable exceptions*)
- Documentation required

3508EZ Form

- Loans over \$150,000
- Borrower certifies FTE changes did not occur during Covered Period (*exceptions apply*)
- Documentation required

3508S Form

- Loans of \$150,000 and less
- Borrower certifies program requirements were met
- No documentation required at the time of forgiveness application



Polling Question #3

Did you opt into the SBA direct borrower forgiveness program?

A. Yes

B. No

Approaches for Simplifying Forgiveness Applications

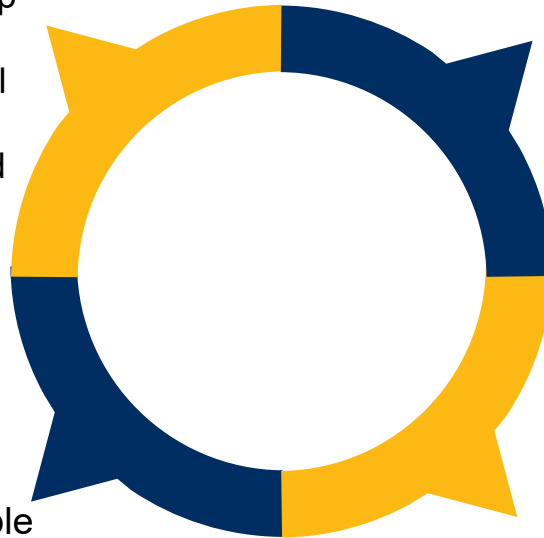
In general, the fewer cost categories listed on your forgiveness application, the less documentation required to support your forgiveness request. Below are some strategies for simplifying your forgiveness application and reducing the amount of SBA required documentation.

1. Extend the Covered Period

If you extend your Covered Period beyond 8 weeks (up to at most 24 weeks), you may be able to accumulate enough employee compensation costs to cover the full amount of your loan. If so, you can simplify your forgiveness application by only submitting the required documentation for those compensation costs.

3. Achieve Full Forgiveness with only Employee Compensation

With a longer Covered Period, borrowers may be able to accumulate enough employee compensation costs to cover the amount of the loan. In this case, no other documentation needs to be prepared or retained.



2. Limit the Number of Cost Categories Used

You only need to provide supporting documentation for eligible costs sufficient to cover your forgiveness amount, up to the amount of your original PPP loan. In some cases, especially when the Covered Period is extended to 24 weeks, eligible costs may consist solely of payroll costs.

4. Choose the Simplest Cost Categories to Evidence

If full loan forgiveness cannot be achieved solely with employee compensation costs, choose the easiest cost categories to evidence first to limit the amount of documentation required to support your forgiveness request.

1. Employee Benefits
2. Owner Compensation
3. Nonpayroll Costs

Approaches for Simplifying Forgiveness Applications

Along with extending the Covered Period and reducing the number of cost categories, below are other ways to expedite the review process and help the Bank better understand your supporting documentation.

1. Provide Cost Category Summaries

Cost category summaries will help us quickly understand the costs associated with each category on your application. The total in your summary should match the value for that category on your application.

3. Evidence of Costs Being Incurred and Paid

In general, borrowers must provide supporting documentation evidencing that each cost they are requesting forgiveness was both incurred and paid during the Covered Period.



2. Highlight Bank Statements

If bank statements are provided as support of payment of cost categories, please highlight the relevant costs on the statement to make them easily identifiable. If multiple cost categories are on the statement, please make a note on the statement as to which cost the line item applies to.

4. Services and Agreements in Effect Prior to 2/15/20

For non-payroll cost categories, borrowers must provide evidence that the agreements and services were in effect prior to February 15, 2020. This documentation may include account statements from February 2020, a copy of your current lease, or invoices for the month including February 15, 2020.



PPP Lessons Learned

- **What worked:**
 - Lenders showed creativity and flexibility in providing a "new to the world" product quickly and with limited guidance
 - In a matter of days, \$349 billion was distributed to around 1.6 million small business owners
 - Feedback from borrowers was generally positive
 - According to the National Bureau of Economic Research, PPP loans led to a 14 to 30 percentage point increase in a business's expected survival, and a positive but imprecise effect on employment

PPP Lessons Learned

Observations

- Borrowers did not understand requirements
- Lenders were not familiar with all the nuances of PPP
- Limited guidance at first
- No checklists for lenders/borrowers

Rules changes

- SBA lists 30+ Interim Final Rules issued
- SBA lists 10+ Lender Notices issued
- Forms changed and new forms were added
- These changes caused significant confusion
- Already new changes in most recent wave

PPP questions

- Borrowers asked many more questions than lenders anticipated
- Lenders were not always clear on how to answer
- SBA was inconsistent in answers; methodology for communicating, etc.
- Not all borrowers were tech savvy

Lasted longer than expected

- Borrower has 10 months from end of covered period to apply for forgiveness
- Lenders had not anticipated keeping loans on books for longer periods
- SBA questionnaires and loan audits were not anticipated and will continue

PPP Lessons Learned

Processing

- Documentation review was inconsistent (origination and forgiveness)
 - Too much time reviewing documentation
 - Missed issues due to not enough documentation
- Fraudulent loans occurred
 - Industry study indicates ~15% of loans may be fraudulent
- Pipeline tracking was problematic
 - No date stamps to be able to track to SBA requirements
 - Limited audit trails
 - Inability to track back and forth with borrowers
 - No consistent flow of forgiveness requests
 - Difficult to manage the 60-day forgiveness timeline and loan review requests
- Data quality was questionable
 - Names in documents do not match (person vs. Company)
 - SBA mismatches and hold codes to resolve
 - Problems with reconciliation and tracking of data
 - Data governance importance when using systems

Staffing was a challenge

- Tight timeline to originate
- Inexperienced originators—pulled from other departments
- Not enough people dedicated to answer phones and emails
- Forgiving and originating at the same time
- PPP fatigue

What To Do Differently for Lenders

Project Management Process

- People/Process/Technology—all can change at same time
- Set expectations and build in accountability
- Design an efficient process but build in controls along the way
- Be conscious of potential fraud and flag to remove for forgiveness (fast track submission for guarantee)
- Documentation review
 - How much documentation?
 - Support for origination decision and forgiveness recommendation?
 - Reasonableness
- The pipeline
 - Queue: control workflow as much as possible
 - Encourage borrower forgiveness and ongoing messaging
 - Processes and procedures (collections, guarantees, fraud)

Change Management Controls

- Communication and implementation of new regulations/changes
- Respond quickly and timely
- SBA reviews
- Thought we would be done no later than Dec.
- Duration
 - New wave
 - Forgiveness time extended

Internal Audit, Loan Review Compliance

- Utilization
- Ask advice when designing project and change management controls
- Correct as detected if IA finds systemic issue
- Especially if originating new customers, especially with compliance

What To Do Differently for Lenders (and Borrowers)

Communicate Communicate Communicate

- Proactively communicate with borrowers
 - Webinars
 - Emails
 - Webpage
 - Call Center
 - Help Line
 - SBA Direct Portal
- Provide training
 - Origination
 - Forgiveness

PPP Internal Audit Procedures

- Through discussion with management, determine the process management follows to collect completed Paycheck Protection Program Borrower Application Forms along with payroll documentation. Determine if the financial institution is using the final approved version of the Paycheck Protection Program Borrower Application Form (SBA Form 2483 (04/20)). Additionally, determine if controls are in place to review application for potential errors and customer program eligibility prior to advancing the loan for further underwriting and processing. Determine what level of documentation exists to support the application review process that occurred.
- Document the client's control details with respect to the items listed above. Attach copies of the reviewed occurrence to support the control design.

PPP Internal Audit Procedures

- Through discussion with management determine the process management follows to underwrite the loan. Determine controls related to the following are in place:
 - A. Confirmation of Borrower Eligibility (Section III (2)(a) - Section III (2)(b)(iv))
 - B. Confirm Receipt of Application & Borrower Certifications (Section III (3)(b)(i))
 - C. Confirm Receipt of Information Demonstrating That The Borrower Had Employees For Whom The Borrower Paid Salaries and Payroll Taxes On or Around February 15, 2020 (Section III (3)(b)(ii))
 - D. Confirm the dollar amount of average monthly payroll costs for the preceding calendar year by reviewing the payroll documentation submitted with the borrower's application (Section III (3)(b)(iii))
 - E. Borrowers are subject to the institutions BSA/AML Protocols (Section III (3)(b)(iv)(I))
 - F. Confirm loans are approved according to the institutions established loan approval authority.

PPP Internal Audit Procedures

- Through discussion with management determine the process established to collect documentation from the borrower supporting their request for loan forgiveness, along with the borrowers attestation that it has accurately verified the payments for eligible costs. Determine the process management follows to assess the documentation and attestation for eligibility of loan forgiveness in accordance with the rules. Additionally, determine if the institution independently calculates the level of forgiveness, and requires approval before the loan is extinguished.
- Additionally, discuss with management the controls they have established to submit a loan forgiveness purchase request to the SBA for an individual loan or a pool of PPP loans. Discuss the level of documentation that is needed to be included within the request. Also, determine how payment requests are monitored, tracked, and recorded to ensure accuracy.

PPP Internal Audit Procedures

- To submit a PPP loan or pool of PPP loans for advance purchase, a lender shall submit a report requesting advance purchase with the expected forgiveness amount to the SBA. Verify that the population report meets all request requirements and that the report is complete by performing one of the following procedures:
 - reconcile the population report to an independent, reliable source
 - review the report query to verify that the report is designed to pull data from all transaction types and the time period requested.
- Document population report verification results in the Population Complete text field under the Sampling Details section of the procedure. Attach any relevant supporting documentation to the procedure.

PPP Internal Audit Procedures

- Obtain a system generated report of all loans that have received loan forgiveness. Select a sample based on the control frequency and the sampling methodology. For each sample selected, test for the following attributes:
 - A. Determine the proper borrower attestation was received related to the Loan Forgiveness Request.
 - B. The Loan Forgiveness Calculation was accurate based on the rules
 - C. Loan Forgiveness was properly approved.
 - D. The institution submitted the required documentation to the SBA for payment
 - E. The payment for the Loan Forgiveness request was properly monitored and tracked once the package was submitted to the SBA.
 - F. Forgiveness payment was received within 15 days (if applicable).

PPP Internal Audit Procedures

- Regarding the use of “Agents”, through discussion of the control with the client owner and review of one recent control occurrence, assess whether the control meets the following requirements:
 - A. Agents are required to be verified according to Policy.
 - B. Agents are required to be reviewed against the SBA SAMs list.
 - C. An individual is responsible for determining that the fees are within SBA Standard Operating Procedures guidelines for compensation to agents.
 - D. Documentation exists to support the verification activities.
- Document the client's control details with respect to the items listed above. Attach copies of the reviewed occurrence to support the control design.

Helpful Links

Loan Forgiveness Rules and Ongoing Guidance – SBA & Treasury

- Sources: Statutory language; forgiveness instructions and application¹, PPP SBA main page²; FAQs³
- Three general independent parameters impact loan forgiveness
 - Permitted use of funds (“payroll costs” vs. “non-payroll costs”)
 - Maintaining headcount (AFEEM = average full-time equivalent employees per month)
 - Maintaining wages of “protected employees” (thresholds)
- Complexity of rules compounded by ongoing nature of guidance

¹ <https://www.sba.gov/document/sba-form-paycheck-protection-program-ez-loan-forgiveness-application-instructions-borrowers>

¹ <https://www.sba.gov/document/sba-form-paycheck-protection-program-loan-forgiveness-application>

² <https://www.sba.gov/funding-programs/loans/coronavirus-relief-options/paycheck-protection-program>

³ <https://www.sba.gov/document/support--faq-lenders-borrowers>

³ <https://home.treasury.gov/system/files/136/Paycheck-Protection-Program-Frequently-Asked-Questions.pdf>

Resources

- **Crowe**
 - PPP Financial Reporting for Lenders
 - 10 Questions Answered
 - Is Your PPP loan forgiveness process set up for success?
 - <https://www.crowe.com/insights/ppp-financial-reporting-for-lenders-10-questions-answered>
 - <https://www.crowe.com/insights/is-your-ppp-loan-forgiveness-process-set-up-for-success>
- **AICPA**
 - Depository Institutions Expert Panel (DIEP)
 - 4 Technical Questions & Answers (TQAs)

9/23/2020 PPP Financial Reporting for Lenders: 10 Questions Answered | Crowe LLP

PPP Financial Reporting for Lenders 10 Questions Answered

7/9/2020

Introduction

Funding for the Paycheck Protection Program (PPP) ended on June 30, in accordance with the *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act). Late on June 30, the Senate passed [S. 4116](#), by voice vote, to amend the CARES Act to extend the program through Aug. 8. On July 1, the House passed the bill by unanimous consent. On July 4, President Trump signed the bill into law, officially extending the program for another five weeks.

On June 30, the American Institute of CPAs (AICPA) issued three [Technical Questions and Answers \(TQAs\)](#), Section 21.30.42-44, to address the following financial reporting questions:

- 42 Classification of Advances Under the Paycheck Protection Program
- 43 Consideration of the SBA Guarantee Under the Paycheck Protection Program
- 44 Accounting for the Loan Origination Fee Received From the SBA

The TQAs were developed by the AICPA's Depository Institutions Expert Panel (DIEP) and cleared by the AICPA's Financial Reporting Executive Committee (FrREC).

PPP loans and the allowance

Q1: Should the lender account for the advance under this program as a loan or as a facilitation of a government grant?

Master Glossary – Loan¹

<https://www.crowe.com/insights/ppp-financial-reporting-for-lenders-10-questions-answered>

Q&A Section 2130

Paycheck Protection Program (PPP)

The CARES Act, as amended, established the Paycheck Protection Program (PPP). The PPP involves a loan designed to provide a direct incentive for small businesses to keep their workers on the payroll. The following questions and answers address certain accounting matters for that program for lenders. Please refer to the [SBA website](#) for detailed information regarding the PPP.

42 Classification of Advances Under the Paycheck Protection Program

Inquiry— Should the lending institution account for an advance under this program as a loan or as a facilitation of a government grant?

Reply— The instrument is legally a loan with a stated principal, interest, and maturity date. The institution is expected to collect amounts due from either the borrower or the Small Business Administration (SBA) as guarantor. The institution should account for this instrument as a loan.

43 Consideration of the SBA Guarantee Under the Paycheck Protection Program

Inquiry— Is the guarantee from the SBA considered "embedded" as opposed to a "freestanding contract" and, thus, can it be considered in estimating credit losses on the loan?

Reply— The SBA guarantee exists at the inception of the loan and throughout its life and was not entered into separately and apart from the loan. If the loan is transferred, the guarantee transfers with it. The arrangement does not contemplate the loan existing without the guarantee unless it is ultimately determined the lender violated an obligation under the agreement. The guarantee was not entered into in conjunction with some other transaction and is not legally detachable. As a result, for institutions that have adopted FASB Accounting Standards Update (ASU) No. 2016-13, *Financial Instruments—Credit Losses (Topic 326): Measurement of Credit Losses on Financial Instruments*, the guarantee would not meet the definition of a *freestanding contract* as defined by FASB Accounting Standards Codification (ASC) 326-20-30.

FASB ASC 326-20-30-12 requires credit enhancements that mitigate credit losses (other than those that are considered freestanding contracts) to be considered in estimating credit losses. The guarantee is considered "embedded" and would, therefore, be considered when estimating credit losses on the loan.

AICPA & CMAA
© 2020 Association of International Certified Professional Accountants. All rights reserved.
For information about the procedure for requesting permission to make copies of any part of this work, please email cpa@aicpa-cma.org with your request. Otherwise, requests should be written and mailed to the Permissions Department, 230 Leigh Farm Road, Durham, NC 27707-8110.

<https://www.aicpa.org/interestareas/frc/recentlyissuedtechnicalquestionsandanswers.html>



Recent Trends in Financial Institution Fraud

Presented by Stacia Schacter



Agenda

- Fraud Statistics
- Internal Fraud Red Flags
- Mortgage Fraud
- Recent Fraud Schemes



Fraud Statistics



Impact of Fraud on Financial Institutions

- Hard to measure
- No one universal definition of fraud = various interpretations
- No one agency that is responsible for investigating fraud

Additionally, many fraud losses are misreported.

Why does this occur?

Because most institutions don't recognize when a fraud has occurred and chalk it up to a bad underwriting decision or another form of operational expense.



Cost of Fraud

Other less-quantifiable costs of fraud to the organization:

- Reputation risk to financial institution
 - Customers trust us with one of their most significant possessions: their money
 - Reputation risk is difficult to quantify
- Increased regulatory focus
- Morale impact on employees



Suspicious Activity Reports

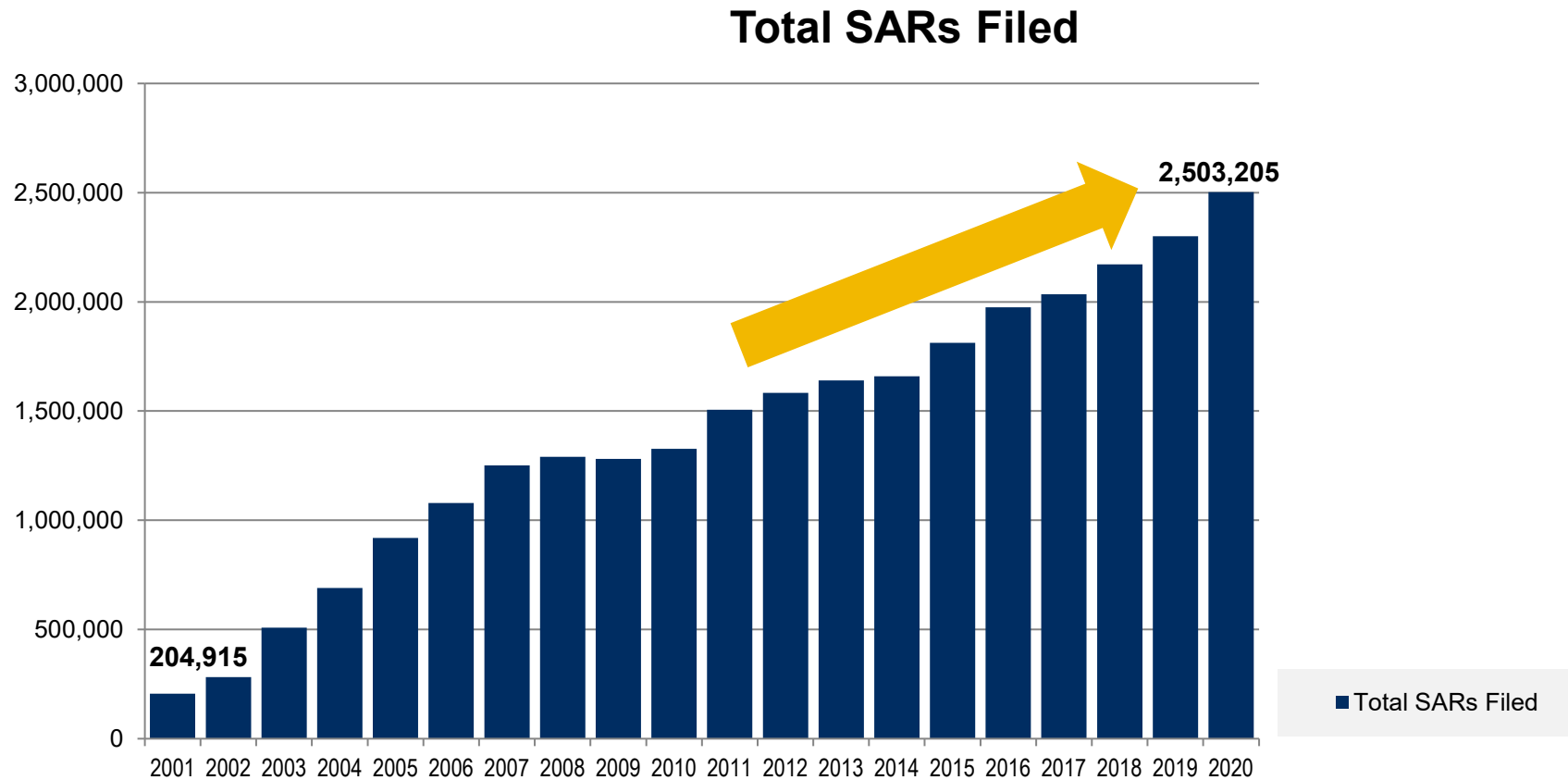
- The Bank Secrecy Act (BSA)
- Regulations require that financial institutions file Suspicious Activity Reports (SARs)
 - Report known or suspected violations of law or suspicious activity
 - Filed with the Department of Treasury's Financial Crimes Enforcement Network (FinCEN)



Suspicious Activity Reports

- FinCEN compiles statistics based on the filed SARs to identify trends and patterns for use by not only the financial institutions but also by law enforcement
- Multiple types of financial institutions are required to file SARs:
 - Depository Institutions
 - Money Service Businesses
 - Securities Sector
 - Others

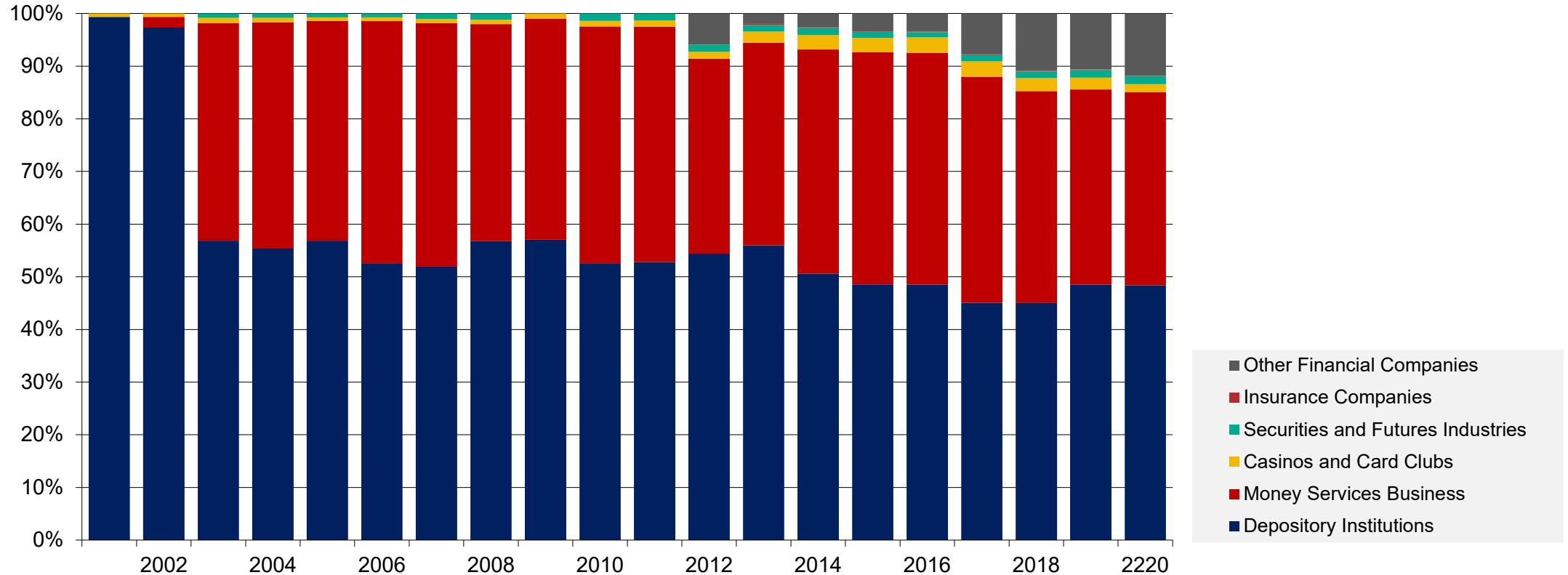
Suspicious Activity Reports



Source: Financial Crimes Enforcement Network (FinCen)

Suspicious Activity Reports

Total SARs Filed by Sector



Source: Financial Crimes Enforcement Network (FinCen)

Cost of Occupational Fraud

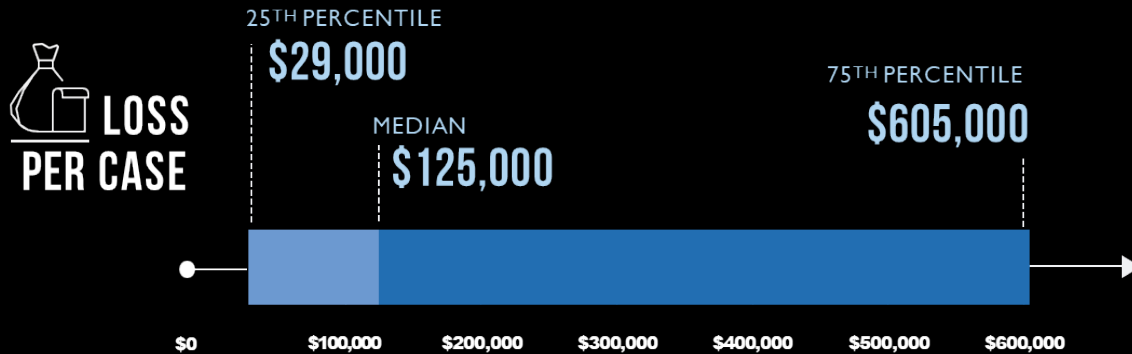
The ACFE's 2020 Report to the Nations reported the following:

- The CFEs who participated in our survey estimated that the typical organization **loses 5% of revenues in a given year as a result of fraud**. To place their estimate in context, if the 5% loss estimate were applied to the 2019 estimated Gross World Product of \$90.52 trillion, it would **result in a projected total global fraud loss of nearly \$4.5 trillion**.
- The total loss caused by the 2,504 cases in our study **exceeded \$3.6 billion**, with an average loss per case of **\$1.5 million**.
- The **median loss for all cases in our study was \$125,000**. **Approximately 21% resulted in a loss of at least \$1 million**.
- Of the 2,504 cases in the study, 386 cases related to the banking industry (the largest reporting sector in the study) with a **median loss of \$100,000**.

Cost of Occupational Fraud

The global cost of fraud.

Fraud is a global problem affecting all organizations worldwide. Because occupational fraud is frequently undetected and often never reported, it is difficult to determine the full scope of global losses. But our data provides insight into the enormity of this issue.



OUR STUDY COVERED
2,504 CASES
from
125 COUNTRIES



Causing total losses of more than
\$3.6 Billion

AVERAGE LOSS PER CASE:
\$1,509,000

CFEs ESTIMATE THAT
ORGANIZATIONS
LOSE




MEDIAN LOSS PER CASE:
\$125,000
AVERAGE LOSS PER CASE:
\$1,509,000

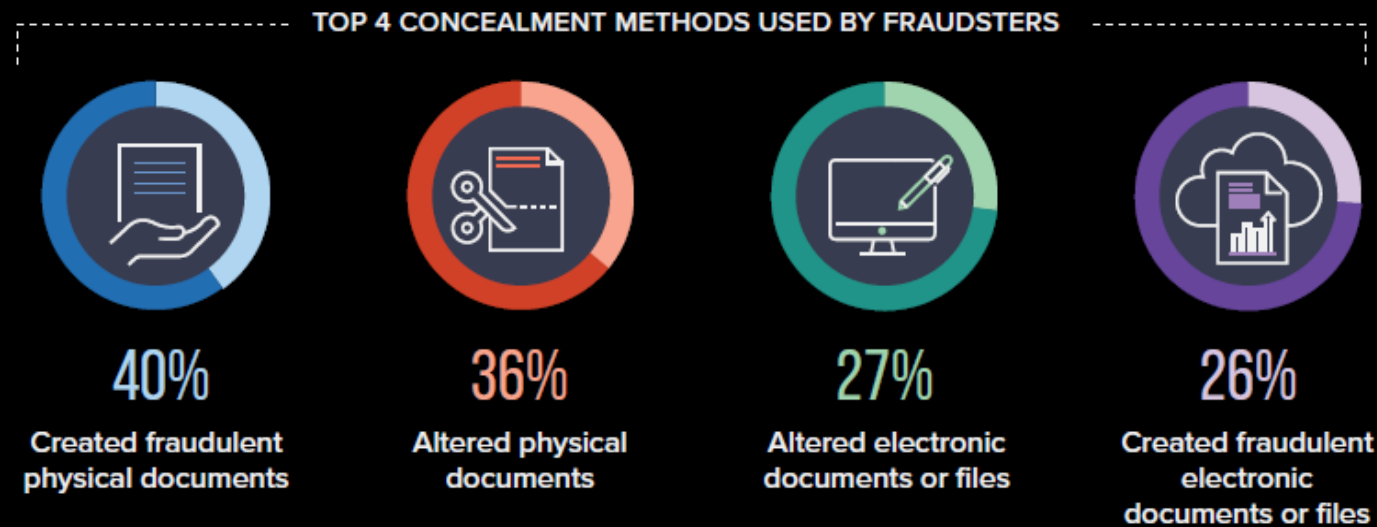
Source: ACFE 2020 Report to the Nations

Concealment of Occupational Fraud

How occupational fraud is concealed.

Understanding the methods fraudsters use to conceal their crimes can assist organizations in more effectively detecting and preventing similar schemes in the future.

 12% did not involve any attempts to conceal the fraud



Source: ACFE 2020 Report to the Nations

How Frauds are Detected

FIG. 9 How is occupational fraud initially detected?

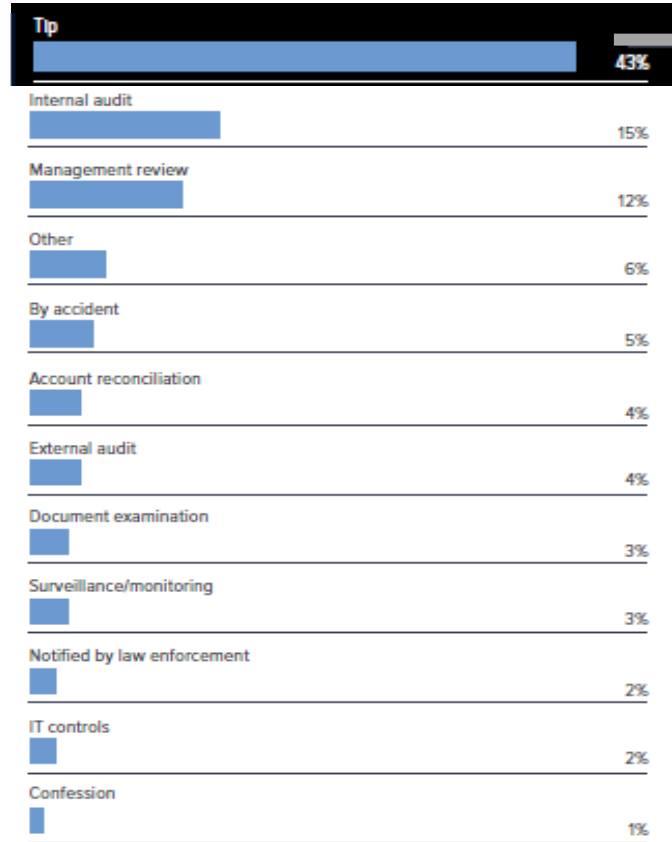
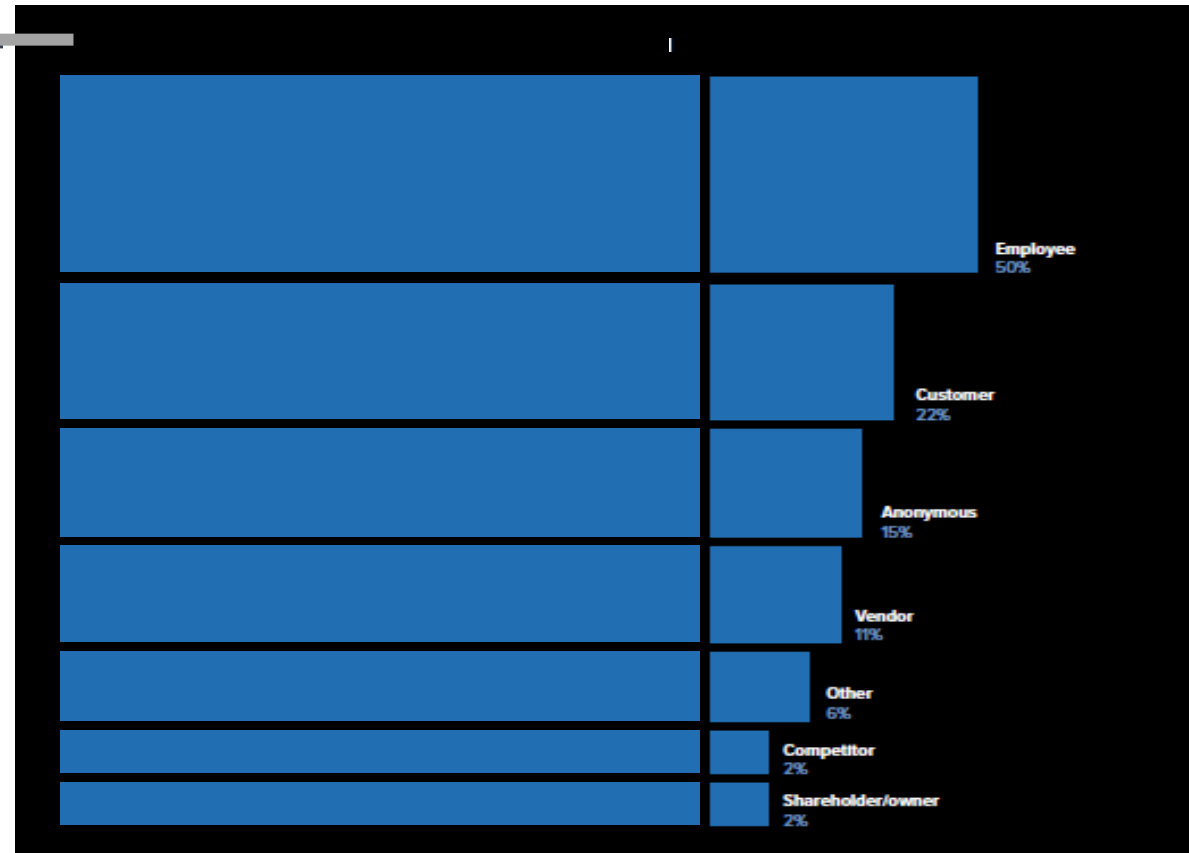


FIG. 10 Who reports occupational fraud?



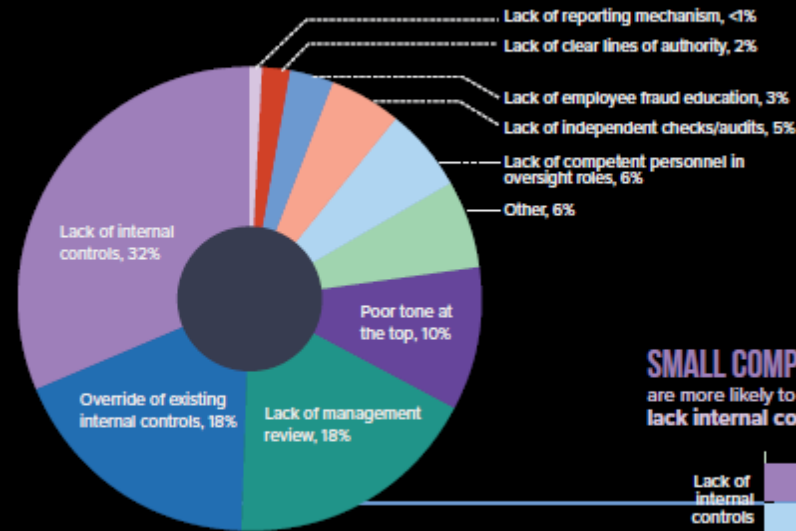
Source: ACFE 2020 Report to the Nations

Causes Related to How Frauds Occurred

Internal control weaknesses that contribute to occupational fraud.

Various factors can facilitate a perpetrator's ability to commit and conceal an occupational fraud scheme.

What are the primary internal control weaknesses that contribute to occupational fraud?



MANAGER-LEVEL PERPETRATORS are more likely than other perpetrators to **OVERRIDE EXISTING CONTROLS**



Employees	15%
Managers	22%
Owner/executives	17%

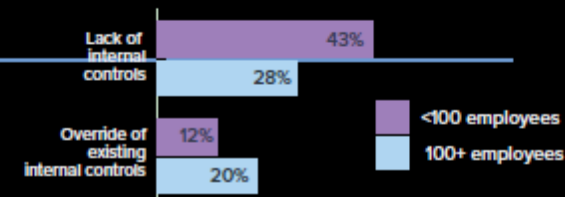
SMALL COMPANIES

are more likely to **lack internal controls**



LARGE COMPANIES

are more likely to have **controls overridden**



Source: ACFE 2020 Report to the Nations

Fraud Losses by Types of Perpetrators

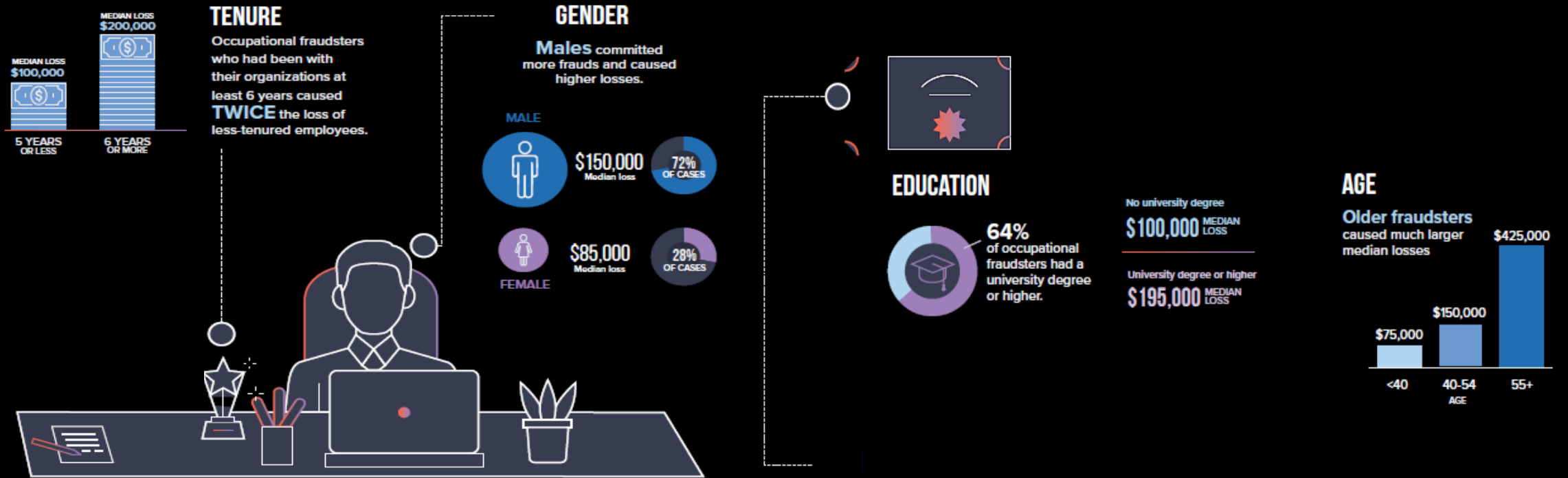
Perpetrator's position.

The perpetrator's level of authority within an organization tends to strongly correlate with the size of a fraud. Owners/executives accounted for only 20% of the frauds in our study, but the median loss in those cases (USD 600,000) far exceeded the losses caused by managers and staff-level employees. This is consistent with our past studies, all of which found that losses tend to rise in tandem with a fraudster's level of authority. Owners/executives are generally in a better position to override controls than their lower-level counterparts, and they often have greater access to an organization's assets. Both of these facts might help explain why losses attributable to this group tend to be so much larger.



FIG. 27 How does the perpetrator's level of authority relate to occupational fraud?

Profile of Fraudster



Source: ACFE 2020 Report to the Nations

Effectiveness of Anti-Fraud Controls



Use of targeted anti-fraud controls has increased over last decade

Hotline	↑ 13%
Anti-fraud policy	↑ 13%
Fraud training for employees	↑ 11%
Fraud training for managers/executives	↑ 9%

A lack of internal controls contributed to nearly



THE PRESENCE OF ANTI-FRAUD CONTROLS IS ASSOCIATED WITH LOWER FRAUD LOSSES AND QUICKER DETECTION



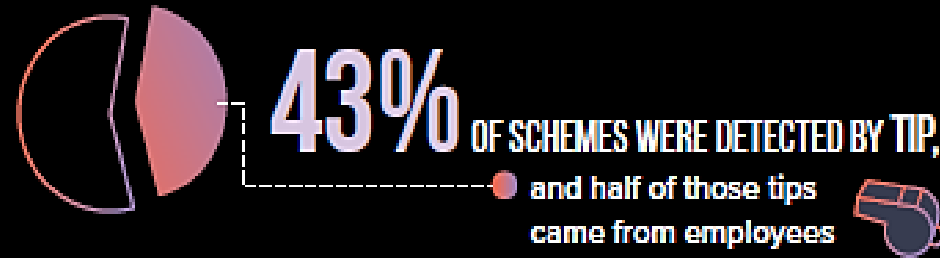
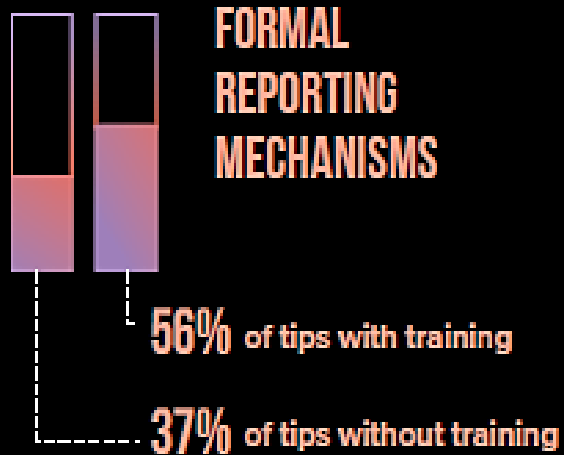
Source: ACFE 2020 Report to the Nations

Effectiveness of Anti-Fraud Controls

Organizations with

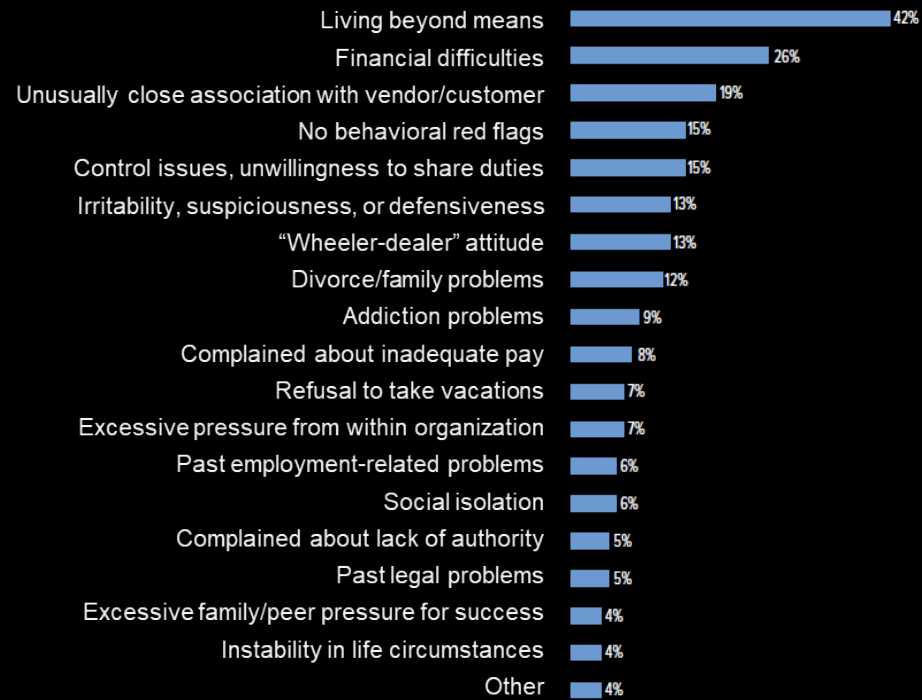
FRAUD AWARENESS TRAINING

For employees were more likely to gather tips through

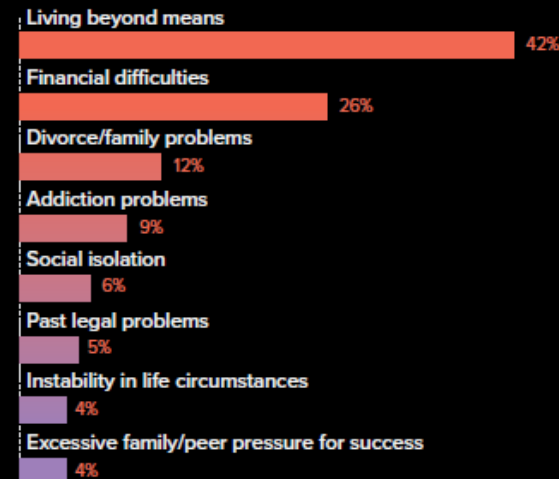


Source: ACFE 2020 Report to the Nations

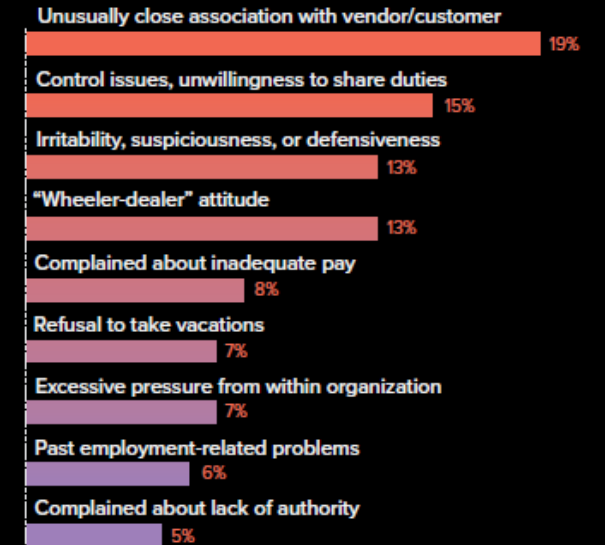
Behavioral Red Flags Displayed by Perpetrators



In **63%** of cases, the fraudster exhibited red flag behavior associated with his or her **personal life**.



In **52%** of cases, the fraudster exhibited red flags connected to their **work duties**.



Source: ACFE 2020 Report to the Nations

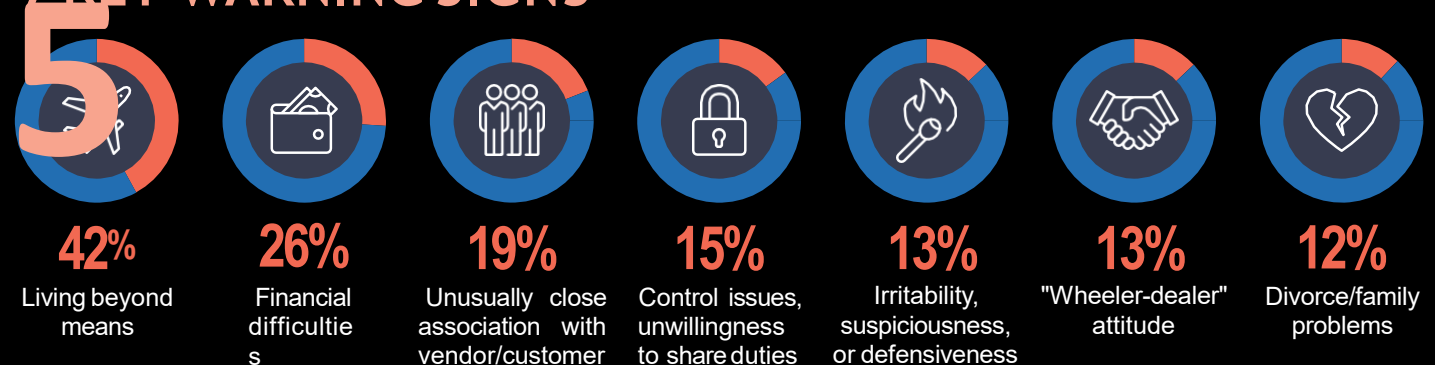
Behavioral Red Flags Displayed by Perpetrators

Behavioral red flags of fraud.

Recognizing the behavioral clues displayed by fraudsters can help organizations more effectively detect fraud and minimize their losses.

8 % OF ALL FRAUDSTERS displayed at least one **behavioral red flag** while committing their crimes.

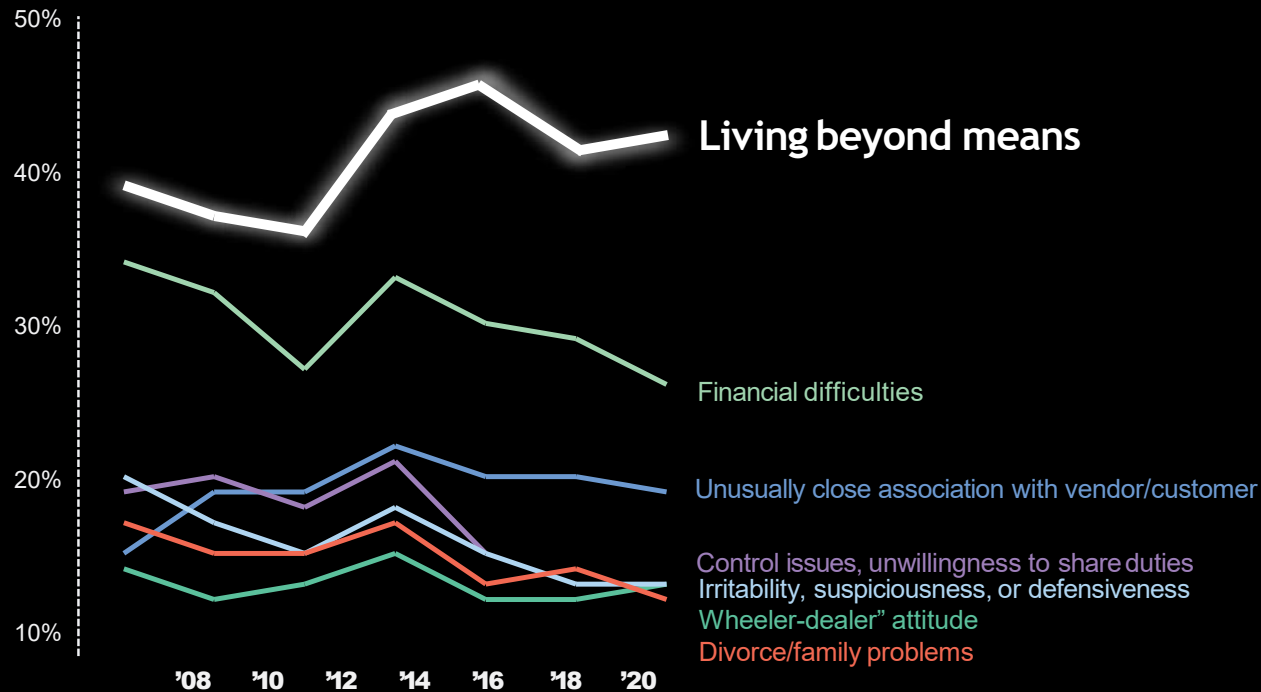
7 KEY WARNING SIGNS



Source: ACFE 2020 Report to the Nations

Behavioral Red Flags Displayed by Perpetrators

LIVING BEYOND MEANS



A fraudster living beyond his or her means is the most common red flag by a sizable margin. This has ranked as the **#1 red flag** in every study since 2008.



Source: ACFE 2020 Report to the Nations



Internal Fraud Red Flags

Fraud Pentagon™

Today's fraudster is clever, cunning, and operating in an environment ripe for criminal activity.

Economic unrest is making it easier for skilled employees to find ways to set fraud in motion--and they are finding cunning ways to do so.

Senior management has to take an offensive stance against fraud and have a clear plan to minimize the impact when fraud does occur. The fraud triangle developed by Donald R. Cressey has now morphed into a Fraud Pentagon™.



Five Elements of the Fraud Pentagon™

- Knowing what may provoke an employee, even an otherwise lawful individual, to blur the line between legal and illegal activity is the key to effectively fighting fraud.
- Famed criminologist Donald R. Cressey first identified three elements - **opportunity, pressure (or motivation) and rationalization** - as the “fraud triangle” in the 1950s to explain why people commit fraud.
- Fraud is more likely to occur when someone has an incentive (pressure or motive) to commit fraud, weak controls provide the opportunity for a person to commit fraud, and the person can rationalize the fraudulent behavior (attitude).

Five Elements of the Fraud Pentagon™

In today's world, we have to expand the fraud triangle to a five-sided Fraud Pentagon™, where an employee's skill and arrogance must be factored into the conditions generally present when fraud occurs.

- Skill is an employee's ability to override internal controls, while arrogance is an attitude of superiority and entitlement that believes that the rules and controls do not apply.
- Talent and confidence play a major role in determining whether an employee today has what it takes to see fraud through.





Five Elements of the Fraud Pentagon™

- Unchecked, these five elements—pressure, opportunity, rationalization, skill and arrogance—can provoke employees to commit fraud.
- **Skilled staff** with widespread **access to bank information**, a **mindset of entitlement**, and the **confidence to pull it off** compound the risk of fraud. Each of these drivers is present to some extent in banks at all times, but never more so than in the current pressure-filled economic environment.



Characteristics: In general, fraud perpetrators tend to be:

- In a position of trust
- Mostly high school educated
- Females versus males
- Have a family/children
- Involved in Community/Charity
- Motivated-often by some need
- Able to rationalize actions



Characteristics: Compared to other types of crime, white collar criminals are:

- A higher percentage of women than men
- More affluent
- Older
- More likely to be married
- Less likely to have used alcohol/drugs
- Had more children
- Heavier
- Completed more grades in school
- More likely to be church members

Source: “How to Detect and Prevent Business Fraud” Albrecht

Conditions Conducive to Fraud

- Weakness in the system of internal control -- segregation of duties and management overrides
- Independent and domineering individuals -- “nerves of steel”
- Weakness in management abilities of senior officers
- Poor maintenance of records in file storage areas
- Lack of effective internal audit
- Limited or no review of employee accounts
- Lack of Board involvement or weak Audit Committee
- Poor staff morale or high turnover
- Incomplete or missing documentation

Conditions Conducive to Fraud

- Unusual relationship between borrower and respective loan officer
- High levels of personal indebtedness by employee
- Accounts which do not balance, such as “suspense”, “official checks”, “cash items” or “clearings”
- Accounts which are force balanced and which have high volume of activity
- Decisions made by one dominant individual
- Out-of-area lending
- Frequent deviation from policies, procedures or common practices - lots of exceptions

Polling Question #1

Which of the following conditions are conducive to fraud?

- A. Accounts which do not balance, such as “suspense”, “official checks”, “cash items” or “clearings.”
- B. Accounts which are force balanced and which have high volume of activity.
- C. Decisions made by one dominant individual.
- D. All the above.

Fraud “Red Flags”

- Unusually high personal debts
- Living beyond one’s means
- Excessive gambling habits
- Alcohol problems
- Drug problems
- Feeling of being underpaid
- Feeling of insufficient recognition for job performance
- Poor credit rating

Fraud “Red Flags”

- Consistent rationalization of poor performance
- Wheeler-dealer attitude
- Intellectual challenge to “beat the system”
- Criminal record
- Not taking vacations of more than two or three days
- A department that lacks competent personnel
- A department that does not enforce proper procedures for authorization of transactions
- No separation of duties between the accounting functions



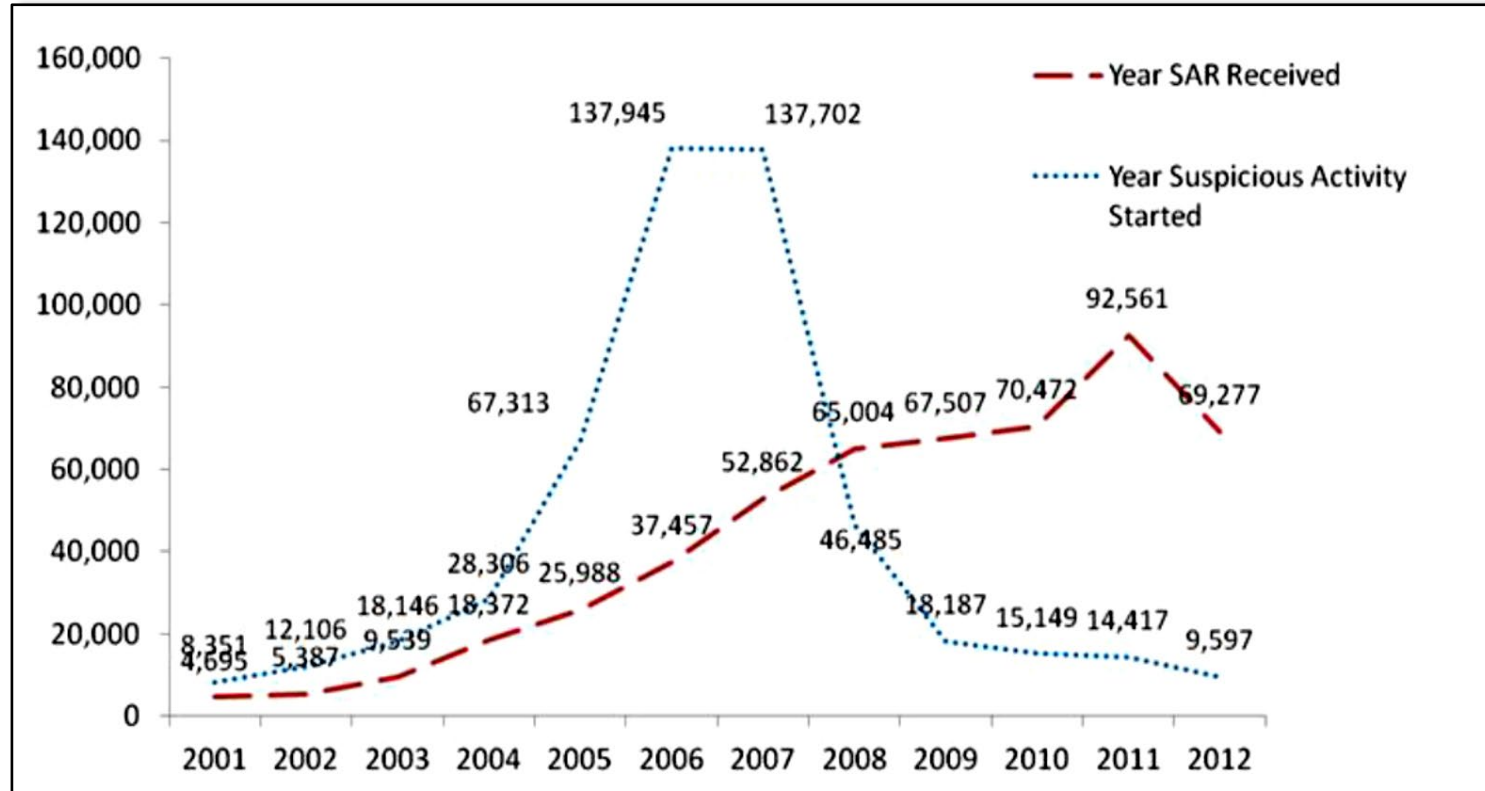
Fraud “Red Flags”

- No explicit and uniform personnel policies
- Inadequate attention to details
- Placing too much trust in key employees
- Pay levels not commensurate with the level of responsibility assigned
- Failure to discipline violators of company policy
- Not adequately checking background before employment



Mortgage Fraud

Mortgage Fraud Trends—SAR Filings (Illustrative Past – Future Predictor)



Source: Financial Crimes Enforcement Network (FinCen)



Mortgage Fraud—Defined

- Mortgage fraud is defined as the intentional misstatement, misrepresentation, or omission by an applicant or other interested parties, relied on by a lender or underwriter to provide funding for, to purchase, or to insure a mortgage loan.
- Mortgage fraud is a relatively low-risk, high-yield criminal activity that is accessible to many.




Mortgage Fraud—Defined

- Finance-related occupations, including accountants, mortgage brokers, and lenders were the most common suspect occupations associated with reported mortgage fraud.
- Perpetrators in mortgage industry occupations are familiar with the mortgage loan process and therefore know how to exploit vulnerabilities in the system.

Mortgage Fraud—Two Categories

- Mortgage loan fraud is divided into two categories: **fraud for property and fraud for profit.**
- **Fraud for property/housing entails misrepresentations by the applicant** for the purpose of purchasing a property for a primary residence. This scheme usually involves a single loan. Although applicants may embellish income and conceal debt, their intent is to repay the loan.



Mortgage Fraud—Two Categories

- **Fraud for profit**, however, often involves **multiple loans and elaborate schemes** perpetrated to gain illicit proceeds from property sales. It is this second category that is of most concern to law enforcement and the mortgage industry. Gross misrepresentations concerning appraisals and loan documents are common in fraud for profit schemes and participants are frequently paid for their participation.



Fraud Risks - Documentation Misrepresentation

- Loan application
 - False employment information and history
 - Income inflated
 - Borrower details either false or altered
 - Debt and debt history falsified



Fraud Risks - Documentation Misrepresentation

- Appraisal
 - Value inflated
 - Key information omitted
 - Appraiser not certified or independent
 - Improper method utilized
 - Property condition falsely disclosed

Fraud Risks - Documentation Misrepresentation



The above photos are from condos that were involved in a mortgage fraud. The appraisal described “recently renovated condominiums” to include Brazilian hardwood, granite countertops, and a value of \$275,000.

Source: Federal Bureau of Investigation



Fraud Risks - Documentation Misrepresentation

- Credit report
 - Report forged or altered
 - Substitution of good borrower information (identity theft)
 - Forged credit references
 - Hacked credit bureau agencies



Fraud Risks - Documentation Misrepresentation

- Deed/mortgage/quitclaim deed
 - Altered to disguise true property owner
 - Lien holder information altered
 - Mortgage amount altered
 - Falsified information helps disguise property flips



Fraud Risks - Documentation Misrepresentation

- Financial information
 - Fraudulent tax returns
 - Fraudulent financial statements
 - Faked CPA representation (through use of stolen or manufactured letterhead)
 - Altered cash flow and income projections



Fraud Risks - Documentation Misrepresentation

- HUD 1 settlement statement
 - Actual parties to the transaction falsified
 - Settlement charges altered
 - False down payment
 - Borrower's signature forged



Fraud Risks - Documentation Misrepresentation

- Title insurance/opinion
 - Property ownership altered
 - Prior and current liens omitted
 - Chain of title altered
 - Legal description altered



Documentation Misrepresentation Red Flags

- Poorly documented loans and appraisals
- Lack of or unsigned borrower financial statements
- Questionable loan disbursement transactions
- Loan funds disbursed to a third party
- Corporate loans with no endorsements or guarantors



Documentation Misrepresentation Red Flags

- Construction draws with no or inadequate inspection reports
- Construction inspections conducted by unauthorized or inappropriate persons
- Lack of independence between the approval and disbursement functions
- No appraisal or property evaluation in file
- One evaluation in file, but appraisal bills for more than one



Documentation Misrepresentation Red Flags

- Unusual appraisal fee (high or low)
- Appraised value for highest and best use, which is different than current use
- Close relationship between the appraiser and lender or borrower



Prevention Techniques

Documentation:

- Direct access to IRS information
- Cross-reference disclosed data
 - Name
 - Social Security number
 - Property ownership
 - Tax records
 - Employment history
- Direct access to public records
 - Liens
 - Recorded sales
- Direct access to state titling records



Prevention Techniques

Borrowers:

- Verify their identity
- Use “knowledge-based” authentication
- Check OFAC Watch Lists
- If a business, perform business credentialing and license credentialing
- Perform appropriate due diligence



Prevention Techniques

Employees:

- Verify previous employment
- Verify education references
- Perform criminal background checks
- Perform credit checks
- Verify against Financial and Law Enforcement Sanctions databases



Prevention Techniques

Vendors:

- Perform business credentialing and license credentialing
- Verify principal owner identification
- Perform owner background check
- Perform/review vendor employee screening
- Verify references
- Perform appropriate due diligence



Recent Fraud Schemes

Recent Fraud Schemes - Business Email Compromise (BEC) Schemes

- **“Romance scams,”** which lull victims to believe that their online paramour needs funds for an international business transaction, a U.S. visit or some other purpose;
- **“Employment opportunities scams,”** which recruits prospective employees for work-from-home employment opportunities where employees are required to provide their PII as new “hires” and then are significantly overpaid by check whereby the employees wire the overpayment to the employers’ bank;
- **“Fraudulent online vehicle sales scams,”** which convinces intended buyers to purchase prepaid gift cards in the amount of the agreed upon sale price and are instructed to share the prepaid card codes with the “sellers” who ignore future communications and do not deliver the goods;
- **“Rental scams”** occur when renters forward a check in excess of the agreed upon deposit for the rental property to the victims and request the remainder be returned via wire or check and back out of the rental agreements and ask for a refund; and
- **“Lottery scams,”** which involves persons randomly contacting email addresses advising them they have been selected as the winner of an international lottery.

Fraudulent ACH Case Study

- A bank customer's laptop was hacked into.
- The person at the customer who inputs ACH transactions happened to look at her queue and noticed a \$47,000 ACH for payroll that she had not input.
- She cancelled the transaction before it processed, so the fraud did not occur. The customer called the bank and was advised to have all of their computers scanned by their IT person.
- The customer did so and found numerous computers/laptops had viruses including the virus that copies password information (including answers to security questions). The customer has since cleaned their computers and installed virus protection software.

Fraudulent Wire Case Study

- A loan assistant received an email from a customer, responded to the email, but forgot to attach the document the customer requested.
- She called him and apologized for not attaching the information. The customer had no idea what she was talking about (i.e. he had not sent the email).
- A few days later, an email wire request for this customer came through. The loan assistant called the customer immediately to ask if he had made the request. He had not, so she did not process it.
- The email had the request and a facsimile signature saved in the signature matched the customer's identically.
- Somehow the fraudster had hacked into the customer's email and was able to send emails from their account as well as obtained bank employee names and email addresses.



Fraudulent Electronic Funds Transfers – Prevention Techniques

- Basic Internal Controls:
 - Customer Verifications (ex. call-backs)
 - Scheduled Transfers
- There are several technology solutions that help banks determine when multiple parties are “on-line” at the same time. Also, “smart systems” are available to look at customer trends/patterns and will highlight unusual activity.
- Increased customer awareness and preventative techniques (security protocols, encryption, malware software, etc.).

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 1

- A **former loan officer** at Colorado East Bank & Trust in Lamar, Colo., has admitted to his role in a **\$1.2 million fraud scheme**.
- Christopher Tumbaga, 37, pleaded guilty to one count of bank fraud and one count of **receiving illegal kickbacks** in exchange for making loans,
- Tumbaga allegedly used his position as a loan officer at the \$776 million-asset Colorado East to help his high school friend and co-defendant Brian Headle finance his real estate development business with fraudulently obtained credit.
- Prosecutors say that Tumbaga secured a \$250,000 line of credit for Headle **based on false information along with more than 14 loans opened under multiple names**. In return, Tumbaga purportedly received more than \$60,000 in kickbacks.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 1 (continued)

- "In order to get bank funds into Headle's hands, Tumbaga **submitted loan documents with falsified information, including fake financial statements** and documents identifying loan recipients as Headle's relatives, as a way to qualify the loans and skirt bank lending limits to single individuals."
- Tumbaga's misdeeds also allegedly include forging the bank president's signature in order to approve a loan and withdrawing \$100,000 from a bank customer's line of credit so that Headle could pay down his bank debts, according to the release.
- Tumbaga's **faces up to 30 years** in federal prison for each of the two counts.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 2

- Citigroup Inc. said that it has discovered at least **\$400 million in fraudulent loans** in its Mexico subsidiary and said employees may have been in on the crime.
- The bad loans were made to Mexican oil services company Oceanografia OCNGR.UL, a contractor for Mexican state-owned oil company Pemex PEMX.UL.
- Oceanografia borrowed from Citigroup's Mexican unit, Banco Nacional de Mexico, known as Banamex, using expected payments from Pemex as collateral.
- In recent weeks, Banamex learned that Oceanografia **appeared to have falsified invoices to Pemex that were collateral for loans**. The bank wrote down about \$400 million of loans backed by the bogus invoices.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 2 (continued)

- Citigroup noted that a Banamex employee had processed the fraudulent invoices that appeared to be from Oceanografia, and said **that it is "not clear how many people were involved in the fraud."**
- "I can assure you there will be accountability for those who perpetrated this despicable crime and any employee who enabled it, **either through lax supervision, circumvention of our controls or violating our code of conduct,**" Citigroup's CFO stated.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 3

- Pennant Management, a Milwaukee investment firm, has said **it invested \$179 million**, on behalf of clients, in securities backed by what turned out to be **bogus USDA-guaranteed loans**.
- In a lawsuit, Pennant said **it bought 26 fake loans from First Farmers Financial**, a Florida firm that had been approved by the USDA to originate business-and industrial-loans through the agency's rural-development program.
- Nimesh Patel, First Farmer's founder, allegedly **forged the signatures** of USDA officials to pass the fake loans off to Pennant.
- Pennant's major complaint is that, unlike other government-backed loan programs, the USDA's programs have **no central transfer agent or database to allow buyers to easily confirm** that they're buying legitimate guaranteed loans.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 4

- A former loan officer at Wilmington Trust in Delaware is facing jail time after pleading guilty to bank fraud.
- Joseph Terranova conspired to extend credit to borrowers **on terms that would not have been approved by the bank**, the Justice Department charged in an indictment filed in April with the U.S. District Court in Wilmington.
- Terranova, who faces a maximum penalty of five years imprisonment and a \$250,000 fine, also was accused of loaning money to customers to enable them to stay current on loans and caused the bank to misreport loans that were past due or troubled.
- "We hope that in bringing these charges and securing a conviction, **others will be deterred** from engaging in similar conduct," U.S. Attorney Charles Oberly III said in a press release.
- Terranova "**concealed the bank's true financial condition by engaging in 'extend and pretend' schemes to keep loans current and to hide past-due loans from regulators and investors,**" added Christy Romero, the special inspector general for Tarp.

Recent Fraud Schemes

Loan Documentation Fraud – Case Study 5

- India's Punjabi National Bank (PNB) disclosed exposure to a loss of just less than **\$1.8 billion** due to **fraudulent loan guarantees** given to famous jeweler Nirav Modi and companies related to his uncle Mehul Choksi. The initial PNB disclosure led to two junior bank officials' arrests and kicked off a scandal that, continues expanding in scale, scope and potential implications.
- In what has been dubbed the biggest fraud in India's banking history, PNB and police have accused two jewelry groups - one controlled by diamond tycoon Nirav Modi and the other by his uncle Mehul Choksi - of **colluding with bank employees to get credit from overseas banks using fraudulent guarantees.**
- Both Choksi and Modi have denied the allegations and lawyers for the two key accused PNB employees in the case have also said they are innocent.



Loan Documentation Fraud Prevention

- Direct Access to IRS Information
- Cross-Reference Disclosed Data
 - Name
 - Social Security number
 - Property Ownership
 - Tax Records
 - Employment History
- Strong Policies/Procedures
- No Policy Deviation, Without Approved Exception Documentation
- Effective Segregation of Duties/Responsibilities

Recent Fraud Schemes

Teller Cash Fraud

- A head teller stole over \$7 million in cash from the cash vault at a \$52-million credit union, forcing regulators to liquidate the 70-year-old institution.
- The teller confessed to stealing the money by walking out of work on a weekly basis with stacks of \$100 bills, sometimes containing as much as \$100,000.
- The teller was able to hide her thefts by making journal entries into the vault cash account whenever there was an audit or cash count by the credit union supervisory committee, and then making adjusted entries after those counts were completed.

Recent Fraud Schemes

Teller Cash Fraud (Update)

- The teller was sentenced to eight years and eight months in prison and ordered to repay the stolen funds, but that is unlikely because she gambled them all away on Ohio River casino boats. She stole \$7 million over 46 months, a total of about \$150,000 every month, or about \$37,000 every week.
- A bond company paid \$2 million of the loss, but about \$5 million had to be written off as an expense.
- The theft bankrupted the \$52 million credit union, forcing it to merge with a larger credit union.

Teller Cash Fraud – Preventative Techniques

Surprise Cash Counts

- Include all cash supplies and cash items (returned checks, food stamps, redeemed bonds, etc.) assigned to the teller.
- Physically count each bill in the teller's possession. For Vault Tellers, physically count all loose bills and large bills (\$50s and \$100s); sample count strapped \$20s, \$10s, \$5s and \$1s ("fan" straps not counted). For any currency in "Fed wrapped" packages, open packages and "fan" bills to ensure legitimacy. For bagged shipments, either verify or control until pick-up and positively confirm with receiver. For bagged coin, "feel" contents (i.e. pennies are smaller than quarters) and verify on a sample basis.
- Balance cash counted back to the general ledger (i.e. the last time the teller actually balanced to the general ledger).

Teller Cash Fraud – Preventative Techniques (continued)

- If the teller was counted at any time subsequent to teller balancing (i.e., the teller balanced to the general ledger at 2pm, but the count was performed at 4pm), physically verify and control any post cut-off work (i.e. actual cash ins and cash outs). Do not rely on teller tape/machine totals, as these can be easily misrepresented.
- On the day following the cash count, ensure Teller Balancing did not make any adjustments to the teller's general ledger cash balance. If so, the individual responsible for performing the surprise cash count should investigate for propriety.
- On the day following the cash count, ensure there are no outstanding "Cash in Transit" on the general ledger for the teller. If there are, follow to ensure propriety.

Recent Fraud Schemes

ATM Jackpotting

- ATM “jackpotting” is a method in which thieves break directly into ATMs, install malicious software or hardware that makes the machines spit out cash.
- Typically use an endoscope — a slender, flexible instrument traditionally used in medicine to give physicians a look inside the human body — to locate the internal portion of the cash machine where they can attach a cord that allows them to sync their laptop with the ATM’s computer. Once this is complete, the ATM is controlled by the fraudsters and the ATM will appear “out of service” to potential customers.

Recent Fraud Schemes

Certificates of Deposit Fraud

- A former branch manager for an Iowa Bank, pleaded guilty last week to selling **more than \$4 million of phony certificates of deposit** to banks, credit unions and other entities, and now the buyers are trying to get their money back.
- A N.H. Credit Union, which bought a \$99,000 CD it thought was issued by the Iowa Bank, is one of about **50 institutions victimized in the scam**. The credit union has filed a civil suit against the \$890 million-asset Iowa Bank.
- The **former branch manager, who worked at the Iowa Bank for 28 years**, confessed to selling the phony CDs, then using two bank accounts in the names of deceased bank customers to launder the proceeds from the scam.

Recent Fraud Schemes

Certificates of Deposit Fraud

- Federal criminal charges were filed against a **47-year-old woman** who was charged with one count of embezzlement by a bank officer for allegedly **stealing hundreds of thousands of dollars from the CD accounts** of customers at a Marshall, Minnesota bank where she worked.
- The charges state that the bank officer embezzled the money for her personal use.
- If convicted, the bank officer faces a potential maximum penalty of 30 years in prison.

Recent Fraud Schemes

Certificates of Deposit Fraud

- A former Bank of America employee in Massachusetts has been sentenced to three to five years in state prison for **stealing more than \$2 million from her clients.**
- Elaina Patterson, **54**, **used her position as a personal banker at a bank branch** in Reading, Mass., to swindle friends, family members and other customers.
- She persuaded family members and friends to invest nearly \$4.5 million in accounts that she claimed carried above-average interest rates of between 10% and 15%. After **issuing fake certificate of deposit receipts** and forms to convince her investors that the accounts were real, Patterson used their money to make payments to other investors and for her personal use.

Certificates of Deposit Fraud – Preventative Techniques

- Ensure the “vault supply” is maintained under dual control.
- Ensure the “working supply” is locked in the vault at night.
- Ensure the “working supply” is assigned to designated individual(s) for accountability. (Note: Normally, CSRs keep the working supply.)
- Someone independent of sales and custody (or dual control) daily/weekly verifies sold items from the working supply.
- For book entry certificates, controls should be in place to ensure that receipts given to customers for purchased certificates are compared to the deposit subsystem.



Recent Fraud Schemes

Fictitious General Ledger Entry

- A former assistant manager pleaded guilty Friday to stealing more than \$525,000.
- The **thirty-year-old** said she stole the funds by **creating fictitious accounts and false teller entries of unauthorized and fraudulent loans, deposits, check disbursements and transfers, in order to divert funds from customer accounts.**
- She also confessed to destroying records to conceal the scheme.

Recent Fraud Schemes

Fictitious General Ledger Entry

- The former **operations manager and head teller** were convicted of **stealing almost \$600,000** by crediting their own accounts from general ledger funds.
- The 35-year-old former operations manager was sentenced to 12 months in prison and ordered to pay \$395,000 in restitution.
- Earlier, the former head teller pleaded guilty to embezzling \$185,000.
- Prosecutors said the employees had control over their own accounts and each woman stole the funds by **depositing money from general ledger accounts into their own checking accounts.**

Recent Fraud Schemes

Fictitious General Ledger Entry – Wire Transfer

- The former senior **VP and CFO** has been being charged with embezzling more than \$339,000.
- Charges were filed against a **56 year old man**, who was accused of wiring money from the general account to a personal account in order to cover stock market losses, according to Jackson County prosecutors.
- If convicted, he could face 20 years in prison.

Recent Fraud Schemes

Fictitious Entry – Line of Credit

- A **vice president and branch manager** of a Laguna Hills branch was sentenced this afternoon to 41 months in federal prison and just over \$1.8 million in restitution for **stealing nearly \$2 million from a customer's account**.
- The branch manager **withdrew money from a line of credit** in the name of a trust that held an account at his bank. To cover up the scheme, he made interest payments on the money supposedly loaned to the trust.
- The branch manager “stole almost \$2 million dollars from a client for **a personal venture where he was trying ‘to hit it big,’**” according to a sentencing memo filed by prosecutors. “Much like gambling, [the branch manager] used the money on a start-up company that he was intimately involved in and where he could win or lose. Like most risky gambles, he ultimately lost it all.”

Fictitious General Ledger Entry – Preventative Techniques

- Effective reconciliation of general ledger accounts:
 - All general ledger balance sheet accounts and in-house deposit accounts should be properly reconciled (the general ledger/in-house deposit account balance agreed to a subsidiary record, reconciling items adequately dated/described and followed to clearance, and the reconciliation form signed/dated by a preparer and approver) on a timely basis. In addition, reconciling items should clear the accounts timely and properly.
- Segregation of Duties
- Effective Supervision

Recent Fraud Schemes

Credit Card Identity Theft Examples

- Six servers at several Washington-area high-end restaurants **stole credit card numbers from customers and ran up a \$750,000 tab** at stores like Gucci and Barney's of New York.
- In New Orleans, a waitress was charged with **selling up to 50 customers' credit card information**. The waitress sold the numbers for **\$220 apiece** to two men who provided her with a machine used to scan the credit cards.
- A Buffalo, N.Y., man was convicted of **hiring several cashiers at local restaurants and a department store to steal customers' credit card information**.

Recent Fraud Schemes

Credit Card Identity Theft - Case Study

- The FBI recently reported that it broke up a credit card gang for allegedly creating thousands of phony identities **to steal at least \$200 million**.
- The fraudsters made **up more than 7,000 false identities** by creating fraudulent identification documents and credit profiles with the major credit bureaus, pumping up the credit of the false identities by providing false information to the credit bureaus about the identities' creditworthiness, running up large loans using the false identities and never paying back the loans. Of course, the higher the fraudulent credit scores, the larger the loans the fraudsters could obtain.
- The fraudsters allegedly used **sham companies, complicit merchants and black-market businesses** to pull off their crimes.
- They purchased millions in gold, expensive cars, electronics and clothing. They set up bank accounts in Romania, China, Japan, Canada, the United Arab Emirates, India and Pakistan to wire millions of dollars.
- The U.S. Department of Justice (DOJ) charged 18 individual **between the ages of 31 and 74** with one count each of bank fraud. Each could be required to pay a \$1 million fine and be sentenced up to 30 years in prison if found guilty.

Recent Fraud Schemes

Credit Card Identity Theft - Synthetic Identity Fraud.

Faking it:

Reports of synthetic identity fraud are increasing by more than 30% a year, according to some estimates. Here's how a fraudster might pull it off.



Recent Fraud Schemes

Debit Card Identity Theft

- In 2015, a gang of international hackers stole approximately **\$1 Billion from over 100 banks over 30 countries** by using malware to take over the banks' internal operations.
- The gang used **phishing and other social engineering techniques to infect bank employee computers**. Once a virus infected a single bank computer, it then spread throughout the bank's internal network giving the gang access to customer data and various areas of bank operation.
- One scheme was to use the gained access to **infiltrate the bank's ATM network and dispense cash remotely**. One bank lost up to \$7.3 million this way.

Example:

- It took **13 hours for eight people to steal \$2.4 million in New York City through 3,000 ATM withdrawals**. The DOJ charged them for belonging to a New York cell of an international operation that stole approximately **\$45 million from two banks by using stolen prepaid debit card data**.
- The attackers are accused of **breaching the card processors' networks**, where they **removed transaction limits from prepaid card accounts** and then encoded numbers swiped from the banks onto magnetic-stripe cards. The people arrested in New York allegedly used the cloned prepaid cards at ATMs.

Recent Fraud Schemes

Identity Theft – Counterfeit Check Fraud

- The most common frauds that employ fake checks **are mystery or secret shopper frauds**. Police and other agencies across the U.S. and Canada routinely issue warnings about this fraud.
- Those operating this fraud contact victims, often by mail, offering jobs as mystery shoppers and enclosing fake checks. After receiving a mystery shopping check in the mail, **victims are directed to deposit the check into their own checking account**, then to mystery shop a retail location, often Walmart (FYI – Walmart never hires Mystery Shoppers!).
- Consumers are told to **wire part of the money from the check they received**, write up a report on their experience at the store, and keep the “remainder” as their pay. For example, if the fake check is for the sum of \$2,500, the victim may be directed to send \$2,100 and keep the “remainder” as pay. **But the checks are fake**, and the victim is simply sending his or her own money to the crooks.

Recent Fraud Schemes

Elements of a Fake Check

Details in this example are fictitious.



Is the company name or address misspelled?

Does the check number match the check number included in the line at the bottom of the check?

Is the check stock flimsy or suspicious?

If the check is for lottery winnings, why is it written from a company and not the state lottery commission?

Does the check have the correct routing number at the bottom for the bank it is supposedly drawn on? Consumers can Google routing numbers now.

Is the check missing the special ink for the MICR code at the bottom?

Recent Fraud Schemes

Identity Theft – Bankcard Fraud

- Three individuals have been sentenced to three years, five months in federal prison for conspiracy to commit bank fraud in connection with their scheme to deposit fraudulent checks.
- The scheme generally worked as follows: the defendants would post advertisements on social media sites, such as Instagram, seeking individuals who had bank accounts with certain financial institutions and were **looking to make “fast cash.”**
- Upon learning of an interested party, the defendants would obtain the **individual’s bank account information—including account number, PIN number, online banking information, and debit card.** The defendants then **deposited checks that had been stolen or were for closed bank accounts** into the compromised bank account, and would withdraw the funds as cash before the financial institution realized that the checks were not valid. In total, **the defendants deposited more than one million dollars in invalid checks into the compromised bank accounts and withdrew over \$600,000 in cash.**

Recent Fraud Schemes

Real Estate Broker Identity Theft - Case Study 1

- The settlement agent receives a message from the buyer's real estate agent **instructing them to release the earnest money** and deposit back to their client. The email gives wire instructions for the buyer's account.
- It later turns out that **the actual real estate agent did not send this message**, though it came from their email address, and even had other attachments relating to the transaction.
- The buyer's real estate agent's **email account had been "high jacked"** and a criminal was watching the email traffic in order to intervene at just the right moment and send their own message via the real estate agent's account. There is no way to distinguish that it is not really from the true real estate agent.

Recent Fraud Schemes

Real Estate Broker Identity Theft - Case Study 2

- The settlement agent sends the real estate agent **wire instructions for the buyer's earnest money** deposit and final funds to close.
- The criminal who has **hacked the email account** then sends amended wire instructions to the buyer from the real estate agent's email address, with a different bank account on it.
- Or, the settlement agent never sent wire instructions to the real estate agent, but the criminal watches the account and at just the right time, emails wire instructions from the real estate agent's account with a title company name on it, with a bank account that is not with any title company. The funds never make it to the settlement agent.

Recent Fraud Schemes

Loan Fraud Identity Theft

- Martin Ross, 52, a senior vice president with Town Square Bank (Ashland, Kentucky) is facing multiple charges **after processing loans for \$1.4 million to fake clients.**
- Ross processed loans through the bank for several fictitious clients. Names were found to be fraudulent through the National Crime Information Center, where the Social Security numbers and dates of birth belonged to other real Kentucky residents.
- Electronic documents were provided by the bank from Ross' computer that **contained a blank deed, which Ross altered to get loans and credit reports that were also able to be altered.**

Identity Theft – Preventative Techniques

- Enhanced customer awareness and training.
- Compliance with Section 114 (Red Flag Guidelines) and Section 315 (Reconciling Address Discrepancies) of the Fair and Accurate Credit Transaction Act (FACT Act). Including monitoring of 26 known “red flags”, grouped as follows:
 - Alerts, Notifications or Warnings from a Consumer Reporting Agency
 - Suspicious Documents
 - Suspicious Personal Identifying Information
 - Unusual Use of, or Suspicious Activity Related to, the Covered Account
 - Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

Identity Theft – Preventative Techniques (continued)

- Multifactor Authentication - Using more than one of the following ways to confirm identity:
 - What you know (user ids, pin numbers, passwords)
 - What you have (card, token)
 - What you are (your fingerprint, retina pattern)
 - Shared Secret—Prompts a user to enter multiple pieces of information that only that user would know (e.g., mother's maiden name, last transaction amount, etc.) (Passmark [RSA], custom solutions)
 - GeoLocation—Confirming that the location from which the user authenticates is consistent with trends or other information on hand about the user
 - Related foot-printing techniques include checking time of day, computer or MAC Addresses, etc. (Passmark, Cyota—both acquired by RSA in 2006)

Phishing Scams

JPMorgan Victim to Email Phishing Scam (American Banker)

- JPMorgan customers were targeted with a phishing scam earlier this week aimed at obtaining online banking credentials.
- Security researchers from the email provider Proofpoint said the "Smash and Grab" phishing campaign tries to lure individuals to click on a malicious link in an email that looks like an authentic message from JPMorgan.
- Even if customers do not proceed to sign into their JPMorgan bank account, the fraudsters try to automatically install the Dyre banking Trojan on their computers to steal passwords from other institutions.
- JPMorgan Chase, which is the top U.S. bank with \$2.5 trillion in total assets, has more than 50 million customers. The bank believes most of the spam was eliminated by fraud filters. Proofpoint reported that about 150,000 emails were sent on Tuesday.

Phishing Scams

TO: CHIEF EXECUTIVE OFFICER (also of interest to Security Officer)
SUBJECT: Consumer Alert
Summary: *E-mails fraudulently claiming to be from the FDIC are attempting to get recipients to click on a link, which may ask them to provide sensitive personal information. These e-mails falsely indicate that FDIC deposit insurance is suspended until the requested customer information is provided.*

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports from consumers who received an e-mail **that has the appearance of being sent from the FDIC**. The e-mail informs the recipient that "in cooperation with the Department of Homeland Security, federal, state and local governments..." the FDIC has withdrawn deposit insurance from the recipient's account "due to account activity that violates the Patriot Act." It further states deposit insurance will remain suspended until identity and account information can be verified using a system called "IDVerify." If consumers go to the link provided in the e-mail, it is suspected they will be asked for personal or confidential information, or malicious software may be loaded onto the recipient's computer.

This e-mail is fraudulent. It was not sent by the FDIC. It is an attempt to obtain personal information from consumers. Financial institutions and consumers should NOT access the link provided within the body of the e-mail and should NOT under any circumstances provide any personal information through this media.

Phishing Scams



Dear Members:

Alert: Fraudulent "Phishing" Scam Email Designed to Look Like it is from AICPA

On Thursday, February 16, 2012, the AICPA became aware of a fraudulent email using an AICPA banner and referencing the recipient's possible involvement in an unlawful income tax refund activity that was sent to numerous individuals, CPAs, non-CPAs and members of the general public.

The fraudulent email is not from the AICPA. The AICPA and CPA2Biz have conducted an intense review of our internal IT systems and, based on our knowledge of this scheme, have concluded that **none of our systems have been compromised.**

Yesterday we posted an alert on AICPA.org and our social media properties. You may want to ensure that your company, employees and clients are aware of this "phishing" email scam. The Better Business Bureau has an overview of the issue on their website. Do not open any attachment or click on any link as the email may contain a virus. Delete it immediately.

While the exact source has not yet been determined, we are actively investigating the situation.

We will share any updates regarding this matter directly on our [website](#).

If you wish to speak with an AICPA member service specialist, call 888.777.7077 and select option 1.

Phishing Scams

OCC Issues Alert on Fraudulent Letters

- The Office of the Comptroller of the Currency issued an alert about fraudulent letters -- distributed via **email, fax, or postal mail** -- involving funds purportedly under the control of the OCC and other government entities.

“The letters may indicate that funds are being held by the Halifax Bank, London, England, and that the recipient will be required to pay a mandatory express service charge to have the funds released,” the OCC said. The letters are “being sent to consumers in an attempt to elicit funds from them and to gather personal information to be used in possible future identification theft.”

The letters also contain forged signatures of former OCC officials and a fictitious email address. The agency emphasized that any document claiming that the OCC is involved in holding any funds for the benefit of an individual or entity is fraudulent. “The [agency] does not participate in the transfer of funds for, or on behalf of, individuals, business enterprises or governmental entities,” the OCC said.

Phishing Scams

ABA Warns Consumers of 'Grandparent Scam'

- ABA issued a press release warning consumers of impersonation scams -- commonly referred to as "grandparent scams" -- where criminals deliberately target older Americans by posing as family members or friends. According to the Federal Trade Commission, more than \$42 million was lost to this type of fraud between 2012 and 2014.
- "Fraudsters have no problem preying on your goodwill to get inside your wallet," said Corey Carlisle, executive director of the ABA Foundation. "They're using social media and internet searches to fabricate convincing stories, so be careful, trust your gut and do your best to confirm who you're dealing with before sending any money."

Phishing Scams – Preventative Techniques

- Never follow a link in an email and reveal personal data. Go to websites independent of the email.
- Use non-internet means (ex. a phone call) to verify a source. In doing so, do not accept a phone number in the email (use outside source).
- Ensure that email firewalls are current and frequently tested.
- Install automated email verification and email filters.
- Adopt user education and training, including periodic testing of employees.
- Cordon off or “sandbox” suspect emails.



Phishing Scams – Preventative Techniques

Verify the Sender

- An email authentication standard called DMARC is being adopted slowly in financial services – 19% of banks use it, according to a study conducted by Return Path, an email security software provider.
- The DMARC protocol provides a set of checks that verify an email truly came from the domain in its address
- Emails that don't check out can be monitored, quarantined or rejected outright, so they don't hit anyone's inbox.

CyberSecurity Threats

Cyber Threat Examples

- **Mobile Malware:** Studies show that more than 90% of malware is likely to be focused on Androids with a “high probability” of the first appearance of a mass “worm” spreading itself through text messages.
- **Medical Identity Theft:** The Ponemon Institute stated that 94% of Medical Organizations that reported in their recent study had a least one data breach in the last two years.
- **Targeted Attacks:** Also know as “Spear Phishing” or “Whaling” will continue to be on the rise. These are sophisticated attacks on “C Suite” and key operational personnel (ex. the Payroll Clerk).
- **Ransom Malware:** Malware designed to “capture” data from individuals and businesses and hold it hostage until a fee is paid.
- **Intercepting Text Messages:** Using malware that can read text messages of others, like authentication codes sent by banks to verify on-line transactions.
- **Hactivism:** Vigilantly data or disruption of service attacks.
- **Cloud Attacks:** Attacks to stored data via cloud technology. This would be “hyper jacking” since thousands of users could be affected.

CyberSecurity Threats

Cyber Attacks Involving Extortion

- The FFIEC recently issued a statement to notify financial institutions of the **increasing frequency and severity of cyber attacks involving extortion**.
- Financial institutions should develop and implement effective programs to ensure the institutions are able to identify, protect, detect, respond to, and recover from these types of attacks.
- Cyber criminals and activists use a variety of tactics, such as **ransomware, denial of service (DoS), and theft of sensitive business and customer information to extort payment** or other concessions from victims.
- In some cases, these attacks have caused significant impacts on businesses' access to data and ability to provide services. Other businesses have incurred serious damage through the release of sensitive information.

Recent Fraud Schemes

Data Breach Case Study

- Capital One Financial suffered a data breach that exposed the personal information of **106 million customers in late 2019**.
- In August 2020, the Office of the Comptroller of the Currency assessed an **\$80 million penalty** against Capital One for its security lapse.
- The assessment highlights how serious a regulatory risk data-integrity issues are — especially those involving cloud computing.
- The **hack was allegedly carried out by Paige Thompson, a former software engineer at Amazon Web Services**, who broke into Capital One's servers in Amazon's cloud through a misconfigured web application firewall. Thompson was arrested and awaits trial on charges of hacking Capital One and 30 other organizations.

Recent Fraud Scheme

Data Breach Case Study (Observations)

- **Update open-source software** - Thompson gained access to the Capital One data through an insecure web application firewall.
- **Restrict data access** - Thompson was an insider: She had worked at AWS on the Capital One account.
- **Strengthen authentication** - Capital One did not use multifactor authentication on back-end systems like the one that was hacked.
- **Have a response plan** - Capital One did respond quickly and effectively to the breach, such that the hacker was caught right away and the data was rapidly secured.
- **Be ready to share incident information** - A court required Capital One to share the report with the plaintiffs' attorneys in a class action.
- **Don't over rely on cloud providers** - Companies can't outsource security to vendors, especially cloud vendors.

CyberSecurity/Data Breach – Preventative Techniques

- Implement a formal and up-to-date cybersecurity program.
- Designate a cybersecurity leader with appropriate authority and resources.
- Inventory, assess, and prioritize IT systems, data stores, vendors and suppliers, and potential cybersecurity risks.
- Employ procedures to detect and contain cyberattacks – not just to prevent them.
- Create and maintain a plan for responding to cybersecurity incidents.
- Use testing, assessments, and continuous improvement as core elements of your cybersecurity plan.
- Institute a cybersecurity culture, coming from the Board down, and integrate cybersecurity into your enterprise risk management (ERM) program.

CyberSecurity/Data Breach – Preventative Techniques (continued)

- Improve education and training across the organization.
- Keep pace with cyber threats; banks must stay aware and inform employees of new threats.
- Prioritize areas in order to allocate the appropriate resources to mitigate the largest risks.
- Explore cybersecurity insurance.
- Evaluate whether employees should be permitted to use personal devices to connect to the network, as this may inadvertently open the Bank to additional risks.
- Utilize the Federal Financial Institutions Examination Council (FFIEC) [assessment tool](#).
- Compliance with all aspects of the Gramm-Leach-Bliley Act (GLBA).

CyberSecurity/Data Breach – Preventative Techniques (continued)

- If a breach occurs, follow FFIEC Guidance - Security Breaches:
 - “Assess the nature and scope of an incident and identify what customer information systems and types of customer information have been accessed or misused.”
 - “Notify its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.”
 - “File a timely Suspicious Activity Report (SAR), and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate law enforcement authorities.”
 - “Notify customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it.”



Ransomware – Preventative Techniques

- Always use antivirus software and a firewall.
- Enable popup blockers.
- Always back up the files on your computer and mobile devices and keep the backups offline.
- Be cautious when opening emails or attachments you're not expecting or from senders you do not know.
- Always avoid suspicious websites.



Polling Question #2

Following this session, do you have a better understanding of fraud risks and prevention techniques?

- A. Yes
- B. Somewhat
- C. Not really



Thank you

Stacia Schacter

Crowe LLP

(202) 552-8051

stacia.schacter@crowe.com

Sarah Schwartz

Crowe LLP

(954) 202-8543

sarah.schwartz@crowe.com

Layne McGuire

Crowe LLP

(404) 442-1624

layne.mcquire@crowe.com

Maddie Stupinski

Crowe LLP

(312) 632-6588

maddie.stupinski@crowe.com

Edden Burshtein

Crowe LLP

(732) 533-4357

edden.burshtein@crowe.com

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. "Crowe" may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. © 2020 Crowe LLP.