White Paper

Automated Dual Verification: Developing Multi-Level Controls to Enhance Security and Risk Management
Market uncertainty and an increasingly rigorous regulatory landscape have financial institutions facing intense scrutiny to reduce the risk of error and fraud. Regulators are requiring additional security measures and segregation of duties, such as multi-level verification (also known as dual control or dual authority), to ensure that proper controls are in place for mission-critical payment systems. This changing security climate places mounting pressure on financial institutions to ensure that effective and robust controls are in place and being utilized through sound business practices.

With Automated Clearing House (ACH) transaction volumes steadily growing year after year, financial institutions must continually re-evaluate their strategies to reduce ACH risk and any associated financial risk due to potential losses from external sources or employee fraud. Examiners and auditors are increasingly concerned about manual verifications and secondary reviews; this concern is also taking root with financial institutions, as they realize their vulnerabilities and potential liabilities in terms of fraud and risk mitigation.

**Multiple-Level Authorizations**

As a growing practice, examiners and auditors view multiple levels of authorization as critical for the protection of consumers, businesses and financial organizations, and important for maintaining the integrity of the ACH network. Furthermore, the scrutiny of risk management and risk mitigation processes for ACH transactions has intensified with the introduction of non-traditional payment applications, including check conversion applications, Internet- and telephone-initiated transactions and international ACH.

By their very nature, the sensitivity of some transactions necessitates a multi-level verification process, that is, requiring that more than one individual approve the transaction before it can be authorized. Large electronic funds transfers, file maintenance and access to encryption keys are typical examples of e-banking activities that would warrant dual controls.

Regulatory agencies, such as the Office of the Comptroller of the Currency (OCC), require that financial institutions ensure their online ACH services comply with current security and operational standards, as outlined by the Federal Financial Institution Examination Council (FFIEC).
Dual Verification – The Pitfalls of Manual Processing

While most financial institutions practice dual verification as a part of their control process, many still engage in some form of manual processing. The reasons for this can be many. Perhaps the financial institution has not been a victim of fraud, which is often the event that triggers an financial institution’s comprehensive internal audit of overall vulnerabilities. Frequently, and particularly with smaller institutions, it can be a resource issue. In other instances, the financial institution falsely assumes that the third-party service provider responsible for their ACH processing manages these verifications.

A Typical View of Dual Verification

Today, dual verification might look something like this: An ACH operations manager stands over an employee as they process a transaction, perform a batch or detail maintenance, put in payment routing information or set up a new customer. The employee then produces a screen shot of the transaction. An operations manager signs off on the paper and files it away. This verification scenario exposes several vulnerabilities and challenges to financial institutions.

Financial institutions need to be able to easily locate and quickly produce documents every time, on every action, when requested. So, what happens in a case of business resumption or disaster recovery, where manual logs and papers cannot be reproduced? There also needs to be a process in place to verify transactional information, catch critical errors and discern whether or not information has been intentionally (internal fraud) or inadvertently (in error) altered on the document or in the system after verification. If financial institutions lack flags and audit logs, it is possible that vulnerabilities and threats might go unnoticed unless notified by an outside party.

Risk Management Systems and Controls

Pamela T. Rodriguez, AAP, CIA, CISA, Executive Vice President of Risk Management and Education for EastPay, Inc, a regional payments association that provides payments education and risk management services to financial institutions and businesses, notes that specific guidance should be focused on risk management systems and control, and information security. Rodriguez confirms that the systems and controls needed for an effective ACH risk management program should include written policies and procedures, strong internal controls, and a risk-based audit program. Adequate policies and procedures should include the following components:

- Clearly defined duties and responsibilities should ensure strong internal controls over transactions, as outlined in ACH Risk Management Guidance OCC 2006-39.
- A summary of the ACH program’s objectives and its role within the financial institution’s strategic plan is needed to promote overall management and compliance.
- Board-approved risk tolerances are needed to outline the types of activities the financial institution may conduct and the types of businesses approved for ACH transactions.
- An ACH credit-risk management program is a necessary and critical component for sound dual control.
- An effective vendor management program, including a due diligence process for selecting third-party service providers and an oversight process for monitoring them, is vital to protecting the financial institution’s overall risk position and reputation.
Taking a more granular look at Notification of Change (NOCs), return items, file originations, customer set-ups and file reversals can highlight potential vulnerabilities to all parties in the ACH transaction chain.

**RDFI Exposure**

Management on the Receiving Depository Financial Institution (RDFI) side should pay close attention to their institution’s Notification of Change practices. As zero dollar entries, NOCs cannot be controlled in the balancing process. Without a dollar value attached, NOCs can be easily (and mistakenly) overlooked as a potential risk.

For example, the NOC could be altered to re-route money via fraud (internal/employee fraud) by changing the payment instructions from the intended destination to a new fraudulent destination. Future payments to the original intended destination would then be unknowingly rerouted to the fraudulent destination.

NOC controls should include dual authorization, such as management review and approval for codes to change an account number. To that end, it is important for financial institutions to ask these questions:

- How are we monitoring and controlling NOCs?
- What compensating controls do we have in place to mitigate the risk associated with changing that account number?

**Information Security**

According to Rodriguez, at a minimum, a financial institution’s information security program should address:

- Customer access: financial institutions should ensure dual control and confidentiality in the initial setup and activation of new customers across all channels; also, they should secure the distribution and reset process for any authenticators used to access ACH services.

- Employee access: financial institutions should minimize and monitor the number of personnel with access to systems that support ACH services as well as minimize and segregate ACH staff and limit access to various maintenance and transaction support functions.

- Data security: financial institutions should ensure that sound, risk-based data security controls exist across all ACH-related systems, applications and processes. Control policies and practices should address data in transit and storage. ACH operations staff should accept data only from properly authenticated sources and provide a secure communication channel for all critical or confidential data. Furthermore, financial institutions should identify confidential or critical data used in ACH operations and ensure that proper storage and disposal practices are used.
The answers to these questions will shed significant light on the financial institution’s current controls and its ability to mitigate NOC risk.

Another major area of concern for an RDFI should be its controls and practices regarding return item processing. Ask yourself these questions regarding return item processing:

- Does our ACH exception item processing staff have the authority to return entries posted to their own accounts? If so, what dual authorization is in place to prevent entries from being returned that really should not be?
- What controls are in place when transmitting a manual return entry?
- Is the ACH exception item processing balanced on a daily basis? How are these types of returns reconciled? Are they reconciled by staff not responsible for the function, specifically, those without access to file controls?
- Are user access rights and user id audit trails reviewed on a regular basis?
- Who manages user access rights? Is this person(s) also involved in the dual authorization process?

Again, answering these questions is critical to developing and maintaining a risk mitigation strategy that protects your customers and your institution.

**ODFI Exposure**

Management on the Originating Depository Financial Institution (ODFI) side faces challenges in developing and enforcing a robust risk strategy. In terms of originating files, it is not a sound practice to enable the same user to create and approve files. It is important for financial institutions to know how ACH files are originated and limit the ability for users to both receive and transmit, as well as update, ACH files. It is important to ensure that staff members that create origination files for internal departments do not also have the capability to originate entries to staff accounts. To eliminate the opportunity for internal fraud, financial institutions need to have compensating controls in place to ensure the file contents have not been modified or inappropriately handled.

**New Account Setup Exposure**

Setting up a corporate customer involves numerous risks and chances for manual error to occur. To avoid issues, financial institutions should verify that all identifying information, including sensitive account information and scheduling, is input correctly and matches the customer’s authorization agreements. Controls should also be in place to protect this information from being compromised or altered at a later date, without instruction from the corporate customer. And, if compromise occurs, financial institutions must have the ability to stop entries from being sent out into the network, as well as procedures to handle retrieval/reversal of the entries to minimize damage.
Exposure from File Reversals and Rejected Files

In terms of reversing files and entries, or managing rejected files, financial institutions need to be aware of how reversing files and entries are created and if the entries are created by the originator, or by the ODFI. If the ODFI creates the reversing file and/or entry for the Originator, user controls need to be in place to ensure that the contents of the file have not been modified. Financial institutions also need to know who at the ODFI receives the files that are rejected by the ACH Operator and whether the user has update capability.

While these scenarios certainly do not represent a complete list of auditor concerns, or highlight all the areas where fraud can penetrate your organization, hopefully they begin to create a picture of the challenges and complexities surrounding risk mitigation and manual dual verification.

Credible Audit Trails

Manual verification is fraught with pitfalls when an audit process is introduced. In an over-the-shoulder manual dual control scenario, audit trails are virtually impossible to reproduce or manage. If an auditor asks you to demonstrate your control process regarding any of the aforementioned questions, how do you present your case? Because there is no electronic evidence to support a manual paper trail, mistakes or fraud are hard to identify and even harder to analyze.

Operational Costs

When manual dual verification is employed, there is nothing in the payment system to catch manual errors. This can lead to rework, higher costs, reputational risk, NACHA Rules violations and even legal expense. Furthermore, with manual dual control measures, there are two people simultaneously engaged throughout the process—and possibly even a third to trace and correct errors. While necessary for dual verification, tying up multiple individuals to manually perform this process does not lend itself to efficient use of staff resources, and increases operational costs.

So, what is the alternative to manual dual verification? How can a financial institution implement strategies that circumvent many of these challenges without expanding the workforce or reducing the bottom line?

Automated Dual Verification—A Sound Business Practice

Automated dual verification systematically mandates dual approval, which protects both customers and financial institutions. Risk mitigation is enhanced as manual processes are replaced by system security protocols. Audit trails are created that are provable, traceable and reproducible because automated dual verification ensures that the payment process is as it should be and that controls are adhered to. On the operational side, automated verification gives your organization complete control around the core ACH function, adding robust security and validation protocols based on a number of different dual control variables.
Risk Mitigation

Auditor expectations for robust risk mitigation involve implementing and managing a tight control environment that reduces internal and external risks in accordance with institutional tolerance levels and establishes a structured environment for information technology (IT) operations. According to FFIEC, sound IT controls should encompass, “policies and procedures related to personnel and operations, segregation of duties and dual controls, data entry controls, quality assurance programs, industry certification, and operating thresholds and parameters.” Automated dual verification enhances risk mitigation by systemically controlling specific functions, including segregation of duties, dual controls, reconciliations, suspicious activity, and error checks.

Meeting Auditor Expectations

Auditors now expect to see demonstrable, traceable dual verification controls, which makes automated mitigation and dual control processes critical. To be compliant with FFIEC guidance, financial institutions need to have in place:

- Tier I objectives and procedures that seek to identify and manage risks by evaluating the effectiveness of your institution’s and/or your service provider’s wholesale payment systems, internal controls and risk management processes
- Tier II objectives and procedures that seek to verify the effectiveness of the financial institution and service provider wholesale payment systems function by providing additional validation as warranted by the risks

Specifically, auditors will look at institution departmental controls, including separation of duties and dual control procedures, for activities such as notifications of change, funds transfer, clearance and settlement.

Corporate Account Takeover Precautions

Corporate account takeover is a type of business identity theft in which a company’s valid online banking credentials are stolen by criminal entities. It is recommended that financial institutions evaluate their risk profiles with regard to corporate account takeover in order to develop and implement a strategic security plan. This plan should include sound business practices as outlined by NACHA, inclusive for special considerations for RD financial institutions:

- Agreements and minimum security procedures
- Dual control for payment file initiation
- Out-of-band authentication and alerts
- Enhancement of account security offerings
- Exploration of low-tech security options
- Education
Dual Control for Payment File Initiation

It is recommended that an ODFI require payment file initiation under dual control. Dual control involves file creation by one employee with file approval and release by another employee on a different computer.

Dual Verification Approval Rules by User

An efficient automated verification process enables dual control measures down to the operator level. Specifically, operators designated for additional verification should not be allowed to approve pending transactions that they have initiated. In addition, only operators who are not designated for additional verification should be able to approve pending requests and directly update databases. This level of control ensures that error and fraud are mitigated and the audit process is documented and traceable.

Dual Verification Thresholds for Transaction Type and Dollar Amount

With the increasing number and sophistication of ACH transactions, an automated verification process enables financial institutions to set up security control and verification thresholds by transaction type and dollar amount. For example, transaction type thresholds should manage verifications by actions such as additions, deletions or changes, previous verifications and operator security verification. Dollar amount thresholds should be controlled by such variables as the number of verifications required for adding, changing, deleting or approving requests based on the dollar amount of the transaction.

Other thresholds that can be controlled via automated dual verification include daily limit, transaction limit, file limit and multi-settlement date. With this level of control, institutions are more able to manage risk throughout the ACH processing chain.

Reporting and Maintenance Capabilities

Automated dual verification should offer reporting and maintenance capabilities, including reporting functions that prompt users to address pending approval requests. Pending transactions that have not been accepted or rejected are listed for attention. Reporting functionality for automated dual verification provides a critical and systematic audit trail.
Dual Verification from Fiserv

PEP+: Dual Verification from Fiserv delivers a systematic automated solution that ensures and demonstrates that proper controls to mitigate error and fraud in ACH processing are in place. Dual Verification enhances the security and risk management capability of the mission-critical PEP+ application by providing dual verification protocols for specific online request codes. Required authorization is customizable. It can be driven by operator, dollar-amount threshold, or both, and the number of approvals required can vary as needed.

Dual Verification also offers systematic automated tracking and provides a credible audit trail of the secondary review. As a result, it reduces the gaps in risk mitigation associated with manual reviews while increasing operational efficiency. This added layer of security reduces the risk of errors and fraud for financial institutions and their customers.

For more information about how PEP+: Dual Verification from Fiserv can benefit your organization, please contact your Fiserv Account Executive or visit our website at www.fiserv.com/payments.
About Fiserv

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization, and leading the transformation of financial services technology to help our clients change the way financial services are delivered. Visit www.fiserv.com for a look at what’s next, right now.