

TRANSACTION FRAUD WHITE PAPER

The financial industry is facing more aggressive attempts to utilize checks and ACH debits in defrauding banks and their customers. The volume and dollar risk for potentially successful frauds is growing rapidly and has become tougher to identify for reasons such as:

1. Readily available programs for the general public to create professional-looking checks with MICR fonts.
2. Readily available check stock at most computer and office supply stores.
3. The explosion of ACH and Debit Card origination availability and new SEC transaction sets.
4. Merchant/public access to ACH origination services via ISOs for merchant processing services or Internet applications (outside normal banking channels and supervision).
5. Transition to bulk-file, image processing or other non-reviewed payment authorization (non-sight filed item storage) for item handling.
6. No centralized database available to banks for attempted fraudulent items, identifying R/T and account numbers of counterfeited checks or ACH Company IDs for unauthorized items.
7. More participating bill payment providers and increased use of drafts or unsigned payment instruments (such as CheckFree).
8. Promotion of automatic overdraft protection, which pays items into overdraft instead of returning them.
9. Insufficient current detection methods; the fraud is often caught only after the customer questions a transaction that posted on a monthly statement.

A financial institution's ability to implement cost-justifiable ways of identifying potential fraudulent transactions depends on its ability to utilize existing technology and prudent review techniques. Many factors are involved, such as the core system, item processing system, ACH system, transaction volumes, signature verification ability and other review procedures.

Primary Entry Sources of Fraud Transactions

The financial institution opens the door for most fraudulent transactions as it receives and settles payment transactions with external organizations. Generally, checks and payments that are transfers within the bank involve much less risk because they can be reversed or offset using extended deadlines.

Wire transfers, ATM, telephone and Internet/web transactions normally require special review and security authentication and procedures to help minimize the

risks associated with those transactions. Here are the points of greatest exposure:

- **Inclearings:** Paper payments presented by other institutions for daily settlement represent a major source of fraudulent transactions. There is no way to authenticate or verify the signature or approval on each and every item. The 24-hour timeframe for returning items presents the greatest challenge.
- **ACH/Debit Card Debits:** A growing number of ACH payment alternatives and increased availability of origination methods, equipment, vendors and gateways have allowed many more potentially fraudulent transactions into banking channels. Unauthorized “consumer” transactions may be returned up to 60 calendar days after the settlement date, but “commercial” transactions are technically limited to the 24-hour rule.

Originating Depository Financial Institutions (ODFIs) typically bear the bulk of the risks, but Receiving Depository Financial Institutions (RDFIs) can also be exposed to risks and simple customer ill will if a debit is paid and must be returned later. This is especially true if the customer does not reconcile promptly or if the debit causes other valid items to be bounced.

Current Common Identification Methods

Most banks currently rely on these reviews (unfortunately, most occur after the transaction has posted or passed the first line of defense by the bank of deposit/origination):

- **Deposit Review (Reg CC Holds):** This is the first line of defense, where a teller or operations member attempts to identify deposited items that may represent collection risks.
- **Large-Item Review:** The core system identifies items in excess of a floor limit; the bank assigns a staff member to manually review these items for signatures or other indicators of acceptability.
- **NSF/HOLDS/STOP/REJECTS:** As a last line of defense, the items must be postable transactions and not returnable for standard reasons.
- **Charge Backs:** When items are returned, it is often too late because the funds have already been taken.
- **Sorter Rejects:** Hopefully, invalid R/T or non-MICRed items will reject at the bank of first deposit, limiting exposure.
- **Kite Suspects (Debits exceed Opening Balance) Reports:** Often, this report is not even reviewed by the bank.

- **Dormant Activity Reports:** This standard report and review attempts to safeguard inactive accounts from fraud attempts. (Historically, insiders perpetrate most of the fraud that occurs on these accounts.)
- **Signature Reviews:** On sight-paid items, an employee may attempt to compare signatures with card samples on file. However, signature verification is a very subjective review and approval method; employees often go untrained or are unable to easily identify forgeries due to time limitations or slight variations.
- **Customer Notification:** A customer may pre-notify the institution of a potential attempt to defraud their account. Or, after the statement has been sent, notification is either a loss (or ACH return if they are within prescribed time limits).
- **ATM-PIN Authorized Transactions:** If the PIN matches, the transactions are approved and if fraud is involved, cameras or other fraud detection methods are used to attempt to recover the loss.
- **ACH/Debit Card Transactions:** Financial institutions often rely heavily on the customer to review monthly statements in a timely manner and return unauthorized transactions. Merchants may also simply make honest errors that cause double posts.
- **Positive Pay:** Larger customers may use this fraud service, which provides a list of all issued items and amounts to the bank used to approve any payment.
- **ACH Prenote Review:** Some systems provide ACH review reports for prenotes, and some include additional company ID checks in their ACH processing systems to help stop unauthorized transactions from posting.

Common Traits of Fraudulent Transactions:

- **New Accounts:** During the first 90 days, many fraud attempts or losses tend to occur that are initiated by the customer.
- **Large Items:** This is a critical element because of the financial risk involved and the likelihood that a crook will not normally waste time on small dollars.
- **Multiple Signatures Required:** The requirement for multiple signatures increases the risk to the financial institution.
- **Drafts/Unsigned Paper Items:** These paper-based items are presented for payment bearing no signature, an invalid signature, or verbiage indicating that the customer has preapproved the item. Often these items can be identified because they have no check number or signature. (Paper-based items still remain under the 24-hour return rule; the bank may wish to obtain confirmation that the vendor/draft is authorized to make these withdrawals.)

- **Counterfeit Items:** These items have been manufactured by someone other than the customer or an authorized payment processor.
 - The item may have no check number, or it may be a duplicate of an item that has already been paid.
 - The check number will be “out-of-range” from current issued items.
 - The check size, style and appearance will not match the normal item.
 - The signature is printed by a laser printer.
 - The accountholder is a large-balance customer and especially susceptible to fraud attempts, such as a government entity that issues many checks, maintains large balances, does not reconcile in a timely manner and does not use positive pay.
- **Volume Anomaly:** The number of deposits or checks exceeds the historical average number for the customer over a day/week/month period.
- **Value Anomaly:** The total amount of deposits or withdrawals is higher the historical average over a day/week/month period.
- **ACH Fraud:** Incoming ACH debits are not reviewed because the financial industry and NACHA rules place the burden on the ODFI. Reg E allows the RDFI to return disputed CONSUMER transactions for up to 60 days after the date of posting.
 - Many fraudulent transactions will have the same company number associated with all the ACH debits.
 - The ACH Description will be the same/similar for all fraudulent ACH debits.
 - The ACH Description may be somewhat cryptic or generic to persuade the customer that it was a valid item from an existing approved company or transaction.
 - Many disputed items will come from the same ACH batch on the same day (one-time “hit and runs”).
 - The amount may be the same for multiple accounts/customer transactions (“spam and bams”).
 - On single transaction attempts, the amounts will be larger to make it worth the risk to the perpetrator.
 - On bulk transaction attempts, the amounts may be smaller with the hopes that the customer will not reconcile the account, nor bother to dispute due to the hassle.
 - SEC codes such as WEB, POP, TEL, RCK and perhaps PPD are most often associated with suspected fraud transactions since disreputable merchants or crooks typically use them to originate entries.

Enhanced Detection Methods

Banks must utilize technology systems to enhance the detection of suspected fraudulent transactions and proactively notify customers and return items within 24 hours of initial presentment. Here are some ideas that may be incorporated into these systems:

- **Account History Analysis:** Determine transaction history by account for average number of transactions (volume baselines), dollar amounts (value baselines), check number ranges, large item cut-off, or NSF activity.
- **ACH Debit activity Authorizations and Confirmations:** Create per-account ACH transaction files to log the Company ID and confirm authorization for this instance, as well as future transactions by the customer.
- **Customer Notification Alerts:** Send an alert to the customer by their preferred method (mail, email, phone message), informing them that a suspected transaction has been submitted for payment and approval. This can also be used to obtain authorization for Drafts or ACH items received from a company.
- **Customer Issue Range Input:** Allow the customer to tell the bank the range of check numbers being used. The bank would need to be able to support multiple checkbook series in the event of joint accounts or the use of a bill-pay provider that issues paper drafts. This is a modified way of providing a limited positive-pay input for any account.
- **Customer Issued Items Input:** This provides the average customer a way to upload a list of all payments issued and authorized, including the date issued, amount, check number if applicable, and optionally the payee or description. It is a positive pay solution for the average customer.
- **Derogatory File Database:** Identify counterfeit check R/T and accounts, suspected fraudulent ACH Company IDs and ACH Descriptions. A centralized repository could enhance inter-bank sharing of incident reports and updated files.
- **Review Logging:** Establish a means of documenting efforts taken to review suspicious transactions and obtaining approval for audit purposes.
- **Special Handling Account Tracking:** Certain accounts may require special criteria reviews, such as new accounts, two signatures required, special large-balance customers and customer-specific payment approval lists.
- **Large Recurring Payment Logging:** Track instances of recurring large payments so they may be identified in future months after the initial review.

- **Check Order/Reorder Numbers:** Log the check numbers printed and available to the customer.
- **Large Item Review:** View large items and examines them using standard industry review and approvals techniques.
- **Check Style Comparisons:** Compares normal checks against presented items for appearance, size, logos, etc.
- **Anomaly Analysis:** Search for account activity that appears to be inflated in either the number of transactions or the dollar amounts for review. It may also be possible to find items not fitting the historical timing of transactions, such as payroll deposits (Kite and Split Deposit suspects).
- **Secret Mark Verifications:** Have the customer use a special symbol on checks that can be easily verified; this is better than a signature.
- **Draft/Unsigned Item Review:** On items such as CheckFree drafts, secure customer authorization to allow all drafts from this vendor.
- **Duplicate Checks and Out-of-Range Checks:** Items presented that do not fall within a certain range of the recently issued numbers should kick out. Make allowances for multiple ranges for married people or two checkbooks.
- **Unnumbered Items Review:** Similar to the Draft/Unsigned review and Check Style comparisons.
- **POP/ARC/RCK and Original Check Paid:** For ACH transactions used to replace checks, verify that the original item did not already pay against the account.

Benefits of Investment in Enhanced Detection Methods

By incorporating the use of technology to address fraud efforts, the financial institution can reap significant benefits. Some of the most obvious are the following:

- **Reduced Losses:** Every item detected, reviewed and rejected at the gate goes directly to the bottom line. Manual reviews just do not provide significant analysis, and they cannot take advantage of historical transaction patterns on an account-level basis. Fraudulent ACH debit activity is indistinguishable from authorized transactions, unless a database or approval mechanism has been established to verify that the customer legitimately authorized an item.
- **Automated ACH Returns:** On those ACH items that are to be returned, an automated ACH RET file can be created to replace the labor-intensive task of returning them using FedLine, CATIE or another method.

- **Audit Trails:** Physical item review offers no permanent documentation to prove the reviews were completed.
- **Transactional Database:** By creating the analysis of engine to data-mine paper and ACH activity, you provide a better tool to identify customer trends and banking habits.
- **Customer Goodwill:** Stopping fraud before the customer's account is charged and causes other checks to be returned in error can be a huge benefit. Additionally, notifying customers about suspected fraudulent or unsigned/debited items and offering them the ability to advise the institution of issued check ranges or items can be a market differentiator. Customers and potential customers may perceive the institution as more secure and more concerned about its customers than competitors.
- **Marketing Potential:** The transactional database can also provide the ability to perform rifle-shot marketing programs, since the financial institution would be able to find out where customers have their mortgage, insurance and other financial products.
- **Derogatory File Sharing:** There is currently no generally available source for institutions to obtain data about past fraudulent attempts (paper-based or ACH) or companies that perpetrate recurring fraud. It may become possible to create a receptacle for industry fraud information for participating members.

Summary

The vast majority of debit transactions received and paid by financial institutions are received from other payment networks as Inclearings or ACH transactions. Current account agreements either use a "sample signature" or remain silent on the authorization and security methods used to ultimately approve payments.

Changes to item processing and volume growth have made signature reviews unreliable, subjective, or extremely expensive. ACH transactions have essentially defaulted to using Reg E and NACHA's 60-day window for disputed transaction returns, but that eventually results in customer reaction and possible ill will.

Financial institutions now face with more payment methods, easier access to check stock and creation software and expanded ACH debit origination capabilities outside the control of the industry. The use of technology is the best and most logical way to analyze these transactions to identify potentially fraudulent items before the damage is done.