

A Guideline Document on Duplicate Image/IRD Prevention and Detection

Created by the:

CheckImage Collaborative

Raising awareness, promoting the benefits, and encouraging best practices for image exchange and Check 21

December 2006

IMPORTANT INFORMATION ABOUT THIS DOCUMENT: The content of this document was prepared by an informal working group of representatives of various financial institutions, trade associations and check clearing houses. This working group is part of a financial services industry effort to consider issues relating to Check 21 and check imaging.

The working group is co-sponsored by the Electronic Check Clearing House Organization (ECCHO) and the Retail Payments Office of the Federal Reserve Bank of Atlanta. The views expressed in this document are not indorsed by, and do not necessarily reflect the views of, the sponsors or the entities that participate in the working group. This document is not intended as legal advice or opinion or any other form of legal or business recommendation to any person. To the extent that the document identifies or discusses a legal matter, a reader or other user of the document should consult with their legal counsel as to its application to them or to a particular situation.

Duplicate Image/IRD Prevention and Detection

Introduction

With its passage on October 28, 2004, the Check Clearing for the 21st Century Act (Check 21) enabled greater use of imaging technology to improve check clearing. Check 21 creates the opportunity for banks to truncate checks without the agreement of all parties. This is accomplished through the creation of a new legal instrument, the substitute check, which is the legal equivalent of an original check.

The substitute check provides an important transitional vehicle between original paper checks and image exchange. The introduction of substitute checks into the collection process sometimes results in duplicate payments.

The purpose of this document is to provide a guideline to assist institutions of all sizes in the prevention of duplicates, and failing that, in the detection of duplicate payments.

Duplicates can occur in both the forward and return processes providing many opportunities for duplicates to enter the payments stream. This document outlines duplicate prevention and detection processes for creators and receivers of substitute checks or check images.

There are a number of duplicate payment scenarios through multiple payment channels that are the result of unintentional processing errors or fraudulent activities. Duplicate payments can occur as combinations of original checks, substitute checks, check images and ACH converted checks. While there are instances where a duplicate item is legitimate, proper controls can help to detect these items and allow them to be processed normally while preventing inappropriate duplicates from entering the payments system. Each financial institution will need to perform its own process review and risk assessment to determine its appropriate types and levels of protection. This guideline assumes the following:

- Duplicate *prevention* is performed by an institution that truncates the original check and creates either an electronic representation or substitute check
 - The prevention process should also include detection whenever possible
- Duplicate *detection* is performed by an institution that receives either an electronic representation of the check or a substitute check

Duplicate Image/IRD Prevention and Detection

Duplicate Prevention

The responsibility for preventing duplicate substitute checks and images from entering the payment system is borne primarily by the truncating and/or reconverting bank(s). The bank performing the truncation or reconversion function might be the BOFD or a Collecting Bank and the roles of each could be distributed among different institutions - truncating bank, the reconverting bank, the BOFD, or the collecting bank.

The introduction of capture at the Point of Introduction (i.e., Corporate Customer, Teller or Branch), suggests that even tighter prevention methods must be employed since individuals of varied knowledge and skill levels will now become involved in item processing functions. The depository and/or collecting bank will want to be sensitive to duplicate presentments across different transaction types.

Types of Items

An institution that truncates the original check and replaces it with either an image or a substitute check has an obligation to prevent duplicates. Duplicate items can be prevented from entering the payments system by the appropriate entity as follows:

- Forward Collection – As the BOFD, Truncating or Reconverting bank, this represents items received on deposit for collection in either image or substitute check forms.
- Return – As the Paying Bank, this represents items presented for payment but dishonored due to issues with the items or due to account holder status. The return process can also introduce images or substitute check in place of the original check.
- Adjustments - As the Paying Bank that receives a duplicate item, care must be exercised in how the disputed item is resolved in order to prevent an item from being returned in error.

Sources of Duplication

- Point of capture – The increased number of points of capture requires solutions and procedures that can prevent an item that is captured more than once from being introduced into the collection system multiple times. Additionally, procedures are required that provide for the retention of the original check for some specific period but yet ensure that the original check is prevented from entry into the collection system.

Duplicate Image/IRD Prevention and Detection

- ATM – Image ATMs allow for the direct entry of a check for deposit without an envelope. Paper is truncated at the ATM. Requires file level prevention controls.
 - Remote Deposit Capture – Allows for the deposit from a corporate customer to be performed at the desk of a company employee without ever going to the bank. Requires file and item level prevention controls.
 - ACH Accounts Receivable Conversion (ARC) – Checks sent as payments for invoices can be converted into ACH debits. Under NACHA Rules, source documents (checks) must be destroyed within fourteen days of the settlement date of entry. –File and item level prevention controls should be used to prevent duplicates.
 - ACH Back Office Conversion (BOC) - Set for implementation in March 2007. Consumer checks received at a point-of-purchase or a manned bill payment location can be converted into ACH debits. Under NACHA Rules, an image or copy of the check must be retained for 2 years. Requires file and item level prevention controls.
 - Branch (Teller / Back Counter) – Care must be exercised to ensure items are not captured more than once, either as a result of a feeder jam or mishandling. Requires file and item level prevention controls.
 - Reader Sorter – Improper jam handling can create multiple records of the same check. Requires item level prevention controls.
 - Reject Reentry – Incorrect codeline matching and/or jam handling can create multiple records of the same check. Requires item level prevention controls.
- Endorsement Implications – Banks allowing capture at remote points should consider standardized endorsement language that would help identify the “status” of an item, i.e., already truncated. However, there should be some “reversing” language in the event an item must legitimately be processed as an original check. At this time, there are no industry standards to support this process. NOTE: Consideration of implementing this recommendation is possibly too early to gain effective benefit without universally accepted industry operating practices.
 - Software – Issues with applications managing the captured images and the data to create image exchange files and substitute checks for forward collection or return item collection.
 - Substitute Check Printing - Proper software and operational controls are required to prevent duplicate items resulting from exception processing conditions. Consideration should be given to not allow restart of an exception bundle but rather shredding the bundle and performing full reprint.
 - Restarts
 - Jams

Duplicate Image/IRD Prevention and Detection

Methods of prevention

Banks creating image exchange files or substitute checks must examine every aspect of the process from capture to file creation and/or printing. This is to ensure that the creation system and operating procedures provide the appropriate safety and soundness so the account holder is not subject to a loss as a result of a duplicate presentment.

- Validation of output control totals – file and cash letter level.
- Duplicate file checking – check across multiple days within a 5 business day minimum to be considered.
- Validation of first/last substitute check – typical bundle wrapping procedure of checking first and last item of the bundle to that printed on the listing.
- Physical count of substitute checks – software counters in print manager can compare to input file.
- Prior to submission for collection – Collecting Bank
 - Transit Warehouse – implies a repository of all items presented for collection in electronic or substitute check form during the current day as well as from prior days, such as a 5 business day period
 - Additional processes in the collection process add the potential to impede the expedient collection of items due to the timing of search

Prevention “Tools”

Prevention “tools” related to human intervention in various processes can be supplanted by system controls and cannot be ignored. Areas of consideration include:

- Physical Item Handling Procedures
 - Storage
 - Destruction
- Image Quality Assurance (IQA) Failure Recovery Procedures
 - The process for rescanning items that fail IQA should be limited to the scan of an item that matches a previously captured item and not a first time capture of an item.
- Explicit process instructions for paper management from capture to destruction (including item retrieval)
- Operator (sorter, reject reentry, reconciliation, printer) Training

Duplicate Image/IRD Prevention and Detection

Duplicate Detection

The responsibility for detecting duplicate substitute checks and images from impacting the customer is primarily the receiving bank(s). While any financial losses can be recovered from the reconverting bank, the reputation of the receiving bank can still be impacted negatively.

Types of Items

The receiving institution has an obligation to protect its customer, the maker of the check, against duplicate postings and will want to be sensitive to the potential of duplicate presentments across different transaction types.

- Forward collections – As the Paying Bank, this represents possible combinations of items received for payment in the form of a check image, a substitute check, an original check or an ACH debit and may arrive from multiple collection (origination) sources.
- Returns – As the BOFD, this represents the reversal of a deposited item previously presented for collection that has been returned by the Paying Bank. Care must be exercised in resolving adjustments so that its depositing customer is not injured by the actions of others in the process.
- Adjustments – As the BOFD, this represents a potential duplicate that was not the result of any inappropriate action on the part of the depositor, therefore, care must be exercised in resolving adjustments so that its depositing customer is not injured by the actions of others in the process.

Where to detect

The Paying Bank, as the receiver, or the Collecting Bank, as the creator of the check image or substitute check should consider the most appropriate point, or multiple points, in the forward collection process where detection methods could be introduced. Some considerations for duplicate detection points are:

- Prior to posting – Paying Bank
 - o File receipt – exchange agreements will identify the appropriate use of information in headers and records that can be used as one level of checking
 - o On-Us Item Warehouse - implies a repository of all items received that day as well as previously paid items, regardless of source: image, paper, ACH, POS, IRD, Remote Deposit Capture, etc.

Duplicate Image/IRD Prevention and Detection

- After posting
 - EIP (Exception Item Pull) – can identify items presented that day that are exceptions due to duplicate presentments across multiple days. Should be used in conjunction with a Warehouse
 - Fraud system – most fraud systems, particularly positive pay services, include a form of duplicate detection but usually they only apply to a subset of account holders
 - On-Us Item Warehouse - implies a repository of all items posted that day as well as previously paid items, regardless of source: image, paper, ACH, POS, IRD, Remote Deposit Capture, etc.

- Prior to submission for collection – Collecting Bank
 - Transit Warehouse – implies a repository of all items presented/originated for collection that day regardless of source; image, paper, ACH, POS, IRD, Remote Deposit Capture, etc. as well as from prior days.
 - Processes in the middle of the collection process have the potential to impede the expedient collection of items due to the timing of search.

- Other considerations
 - Warehouse requires appropriate identification of items that can legitimately be represented
 - Consider checking across current day and multiple previous days such as a 5 business day history
 - This process can be implemented in two methods:
 - Identified duplicate items are omitted from the posting
 - Identified duplicate items are marked but sent to posting

Methods of detection

Financial Institutions will determine the points and methods of detection that best meet their risk assessments. Each of the following recommended methods of detection should include duplicate checking across multiple days. No standards exist but a minimum of 5 business days should be considered. Potential levels of detection include:

- File level – at the time of receipt and/or file import. Attributes such as file name, time and date of creation and file value are among the attributes to be checked.
- Cash letter – the component of the image file that depicts the sender and the value of a group of items
- Item level – applies to image, paper and other electronic

Duplicate Image/IRD Prevention and Detection

Detection “Tools”

It is not the intent of this Guideline to specify the various processes or software tools available but rather to identify that a combination of the following should be considered to provide the best overall protection. Inherently, the implementation of such “tools” will be an evolving process.

- Software controls
 - File delivery system – the solution used to manage the receipt and submission of files
 - Warehouse application – the solution that maintains a database of transactions across payment channels and performs the duplicate checking to identify “hard” and “soft” hits for review
 - Point of introduction – with the implementation of capture closest to the point of introduction into the collection process (i.e., corporate customer, teller, branch), duplicate checking should be considered a component of the respective point of introduction applications
- Process controls
 - General operating procedures – related to all aspects of paper and electronic handling and specifically as related to exception processes
 - Adjustments – particular care in identifying an item as an adjustment and not a return, especially as it applies to non-conforming IRDs.
 - Point of introduction – particularly important as individuals not trained in item processing functions become part of the process at the corporate customer or branch locations, both domestically and abroad
- Suspect review process - provide adequate information to ensure that false positive conditions can be adequately identified and handled
- Trained staff
 - General knowledge of the paper and electronic process
 - Procedures to handle exception conditions, such as not restarting a bundle when a printer jam occurs while printing substitute checks but rather shredding the existing bundle and reprinting the bundle.

Implications of Undetected Duplicates

Prudent care should be exercised when addressing account holder dissatisfaction. Examples follow:

- Customer account postings – undetected duplicates can result in account overdrafts or not become apparent until the account holder receives his/her statement

Duplicate Image/IRD Prevention and Detection

- Accounting – undetected duplicates can result in accounting implications for the bank through misstated balances, interest not applied, etc.
- Reporting
 - Intra-day customer reporting – undetected duplicates can produce incorrect reporting and result in the over funding of accounts
- Notification – if detection of duplicate substitute checks or images does not occur until after posting, every attempt should be made to provide timely notification of recipients of the duplicates
- Check 21 Warranty and Indemnification – penalties resulting from duplicate items are enforceable by law
- ECCHO Rules and Federal Reserve Operating Circular 3 identify the warranties and indemnifications associated with image exchange. Banks exchanging images under these rules are making warranties that they are not sending duplicate items.

Duplicate Detection Resolution

- Adjustment – industry analysis is currently underway to identify an expedient and consistent process for the resolution of duplicate substitute checks and check images. Institutions should consult their legal council for considerations and directions.

Duplicate Detection Recommendation

Implementation of item level detection systems offer the best overall protection.

Duplicate Image/IRD Prevention and Detection

Summary

This document is intended to highlight the need for prevention and detection of duplicate items in this ever-changing US payments system. New legislation and technologies are allowing rapid change of the manner in which payment collection can occur.

As the industry is faced with declining volume, opportunities to participate in this evolution of electronic collection is extended beyond the bank itself and the use of third-party providers has become prevalent. Therefore, banks using the service of third-party service providers must ensure that system and operational processes are in place to avoid the creation and/or posting of duplicate items. The responsibilities of the BOFD, Truncating and/or Reconverting Bank still reside with a financial institution, regardless of whether a bank performs the processing in-house or uses the services of another entity.

Negative financial impact will result from the improper processing of checks converted to another payment form for collection and/or return purposes. Prudent care must be exercised by all parties to the financial transaction throughout the transaction's life cycle to minimize negative impacts to all affected individuals and institutions.

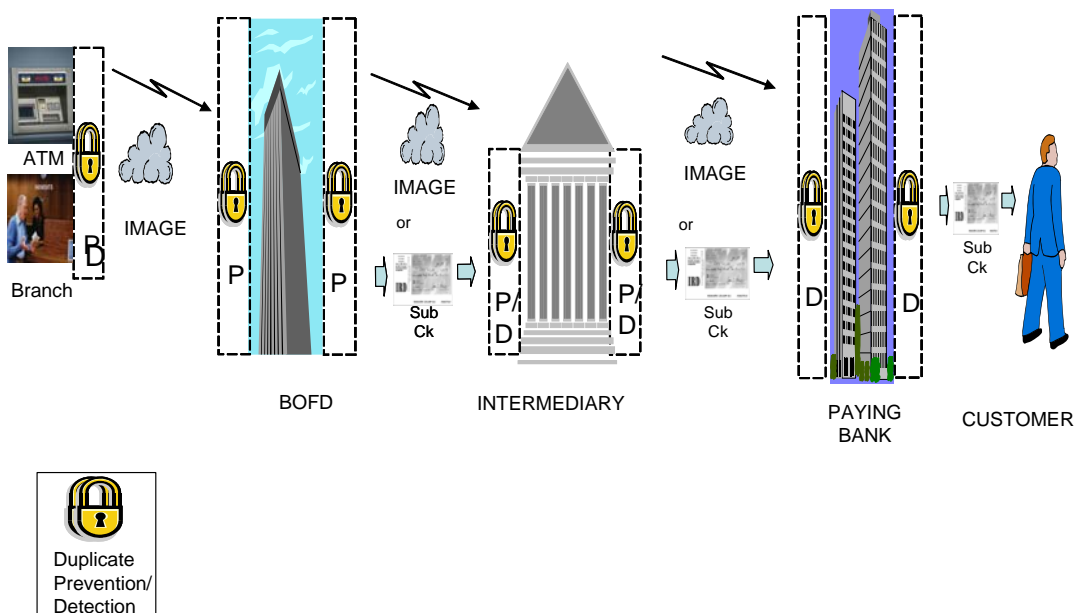
Duplicate Image/IRD Prevention and Detection

Appendix A

Duplicate Prevention and Detection Model

With multiple avenues for duplicates to enter the payments stream, a comprehensive program should be implemented by each entity that is involved in the payments process. The diagram below outlines areas where an institution should consider implementing preventive and detective controls into their operation.

Duplicate – Prevention and Detection



The prevention and detection of duplicates is further complicated by the fact that duplicate items can come from multiple sources - the original check, a substitute check, check images, or an ACH converted check. All of this must be considered as an institution develops a program to prevent and detect duplicates.

Duplicate Image/IRD Prevention and Detection

Appendix B

“Legitimate” duplicates

Since items may legitimately be returned and represented, a capability to recognize these items as non-duplicates needs to be considered. The detection processes will need to allow for certain legitimate duplicates and allow them to process normally. Examples of legitimate duplicates are:

- Redeposited items – those items that were previously presented as forward collection items and returned in either electronic or substitute check form and then subsequently represented for collection should match a prior record at the paying bank. If the representing bank is the same as the original BOFD, the BOFD should also have a record of the earlier deposited items.
- Counter checks – checks that typically do not have a check number can appear as duplicates when the same amount occurs on more than one item
- Rebate checks – checks that typically do not have a distinguishing MICR line attribute but almost always have the same or similar dollar amount(s)
- Stop pays – while a stop pay should not be represented, consider leaving the information available for future duplicate detection events

The establishment of proper controls can help to detect these items and allow them to be processed normally while preventing inappropriate duplicates from entering the payments system.