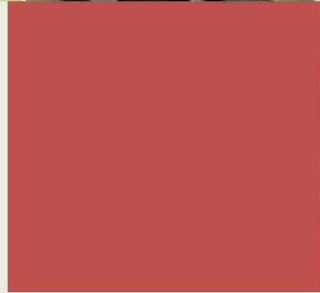




REMOTE DEPOSIT CAPTURE



RULES & TRAINING 2013



T. Houston Technology Group
102 Mustang Drive
Alvin, Texas 77511
281-756-0409
www.thouston.com
Thouston@thouston.com

COPYRIGHT

“Remote Deposit Capture Rules & Training Guide 2013®” is published and printed in the USA and marketed worldwide. Copyright © 2013 by T. Houston Technology Group. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means electronic or mechanical, including photocopying, recording, or by any informational storage or retrieval system without written permission from the publisher, except for brief quotations used in critical articles and reviews. For information contact: T. Houston Technology Group, P.O. Box 1727, Alvin, Texas 77512. Telephone (281) 756-0409 or email: thouston@thouston.com.

For additional project team copies or corporate subscriptions, contact the above numbers, but do not make any additional copies of the book or pages.

ACKNOWLEDGEMENTS

Most people work under the most difficult of circumstances: stress, fear, joy, deadlines, and unreasonable customer demands. We struggle to find balance in our lives. In the Old Testament, a simple shepherd named David had the same problems on his way to becoming the "greatest king of Israel." During his turbulent life, he paused occasionally to write advice about how to handle day-to-day problems. Although these Psalms are thousands of years old, they still bring peace and hope to all that read and believe them.

23 Psalms (King James Translation): The LORD is my shepherd; I shall not want. He maketh me to lie down in green pastures: he leadeth me beside the still waters. He restoreth my soul: he leadeth me in the paths of righteousness for his name's sake. Yea, though I walk through the valley of the shadow of death, I will fear no evil: for thou art with me; thy rod and thy staff they comfort me. Thou preparest a table before me in the presence of mine enemies: thou anointest my head with oil; my cup runneth over. Surely goodness and mercy shall follow me all the days of my life: and I will dwell in the house of the LORD forever.

With the help of many people, we have completed a large part of your homework. The research for this Toolkit required hundreds of hours and we are especially grateful to more people than we can name - but we do want to spotlight a few:

Carter Houston

Mike Reis

Guadalupe McCall

Editor-in-Chief

Western Regional Sales Manager

Writer & Editor

Table of Contents

<u>COPYRIGHT</u>	<u>3</u>
<u>ACKNOWLEDGEMENTS</u>	<u>3</u>
<u>LEGAL REFERENCE DISCLAIMER</u>	<u>1</u>
<u>WHAT’S NEW IN REMOTE DEPOSIT CAPTURE?</u>	<u>1</u>
<u>INSTRUCTIONS FOR USING “2013 REMOTE DEPOSIT CAPTURE RULES & TRAINING GUIDE”</u>	<u>2</u>
<u>REMOTE DEPOSIT CAPTURE WORKPROGRAM</u>	<u>3</u>
TEXAS DEPARTMENT OF BANKING	3
OVERVIEW	3
<u>CHECK 21 ACT AND REMOTE DEPOSIT CAPTURE BASICS</u>	<u>4</u>
WHY CHECK 21 ACT?	4
REMOTE DEPOSIT CAPTURE SYSTEM	4
IMAGE EXCHANGE NETWORKS	5
BENEFITS OF REMOTE DEPOSIT CAPTURE	9
ELECTRONIC SECURITY	12
CONSUMER SENTINEL NETWORK	14
ENCRYPTED TRANSMISSIONS	16
CHECK CAPTURE EQUIPMENT TRENDS	17
<u>CHECK 21 ACT AND REMOTE DEPOSIT CAPTURE WARRANTIES AND INDEMNITIES</u>	<u>19</u>
WARRANTIES	20
INDEMNITIES	21
<u>ABOUT CHECKS</u>	<u>22</u>
SUBSTITUTE CHECKS	23
CHECK ENDORSEMENTS	24
CUSTOMERS CANNOT REQUIRE ORIGINAL PAPER CHECK	26
CHECK CARRIERS	26
IMAGE QUALITY ASSURANCE (IQA)	27
COURTESY AMOUNT RECOGNITION (CAR) AND LEGAL AMOUNT RECOGNITION (LAR)	29
CHECK IMAGE COMPRESSION	31
<u>AUTOMATED CLEARING HOUSE (ACH)</u>	<u>31</u>

ACH AND REMOTE DEPOSIT CAPTURE TECHNOLOGY COMPETE	32
ACH AND CHECK 21 ACT TECHNOLOGY AND LAWS/RULES ARE DIFFERENT	32
ACH TRANSACTIONS FOR REMOTE DEPOSIT CAPTURE	32
RDC & ACH	33
 INTERNAL CONTROLS	 34
 READER’S NOTE: PURPOSE OF THIS SECTION.	 35
REMOTE DEPOSIT CAPTURE OPERATIONS AND RISK MANAGEMENT POLICY	35
STATEMENT OF PURPOSE	35
BACKGROUND	35
RISK MANAGEMENT COMPONENTS	36
PRIVACY OF INFORMATION	37
DOCUMENT AND RESOURCE MANAGEMENT	37
HUMAN RESOURCE MANAGEMENT	38
COMPUTER SOFTWARE PATCH MANAGEMENT	38
LEVELS OF ACCESS RESTRICTIONS	39
INFORMATION TECHNOLOGY SECURITY SAFEGUARDS	39
UNAUTHORIZED ACCESS OF INFORMATION (BREACH)	40
VENDOR OVERSIGHT	41
ALTERNATE DEPOSIT PLAN	42
EMPLOYEE TRAINING	42
AUTHORITY AND REVIEW	42
 REMOTE DEPOSIT CAPTURE PROCEDURES	 43
 AN OVERVIEW	 43
DAILY PROCEDURES	44
PLANNING THE DAY’S ACTIVITIES	45
VERIFY PREVIOUS DAY’S DEPOSIT	46
VERIFY PREVIOUS DAY’S DEPOSIT ACKNOWLEDGEMENT WAS FILED	47
REVIEW SYSTEM AND SECURITY REPORTS	48
PREPARING CHECKS FOR PROCESSING	49
USE ENDORSEMENT PRINTER	50
CREATE A CONTROL DOCUMENT	51
EQUIPMENT MAINTENANCE	52
JOG CHECKS	54
CAPTURE CHECKS	55
VERIFY IMAGE QUALITY	56
DAILY PROCESSING LOG	57
STORE CHECKS IN SAFE PLACE	58
SHREDDING CHECKS	59
DAILY BACKUP AND ARCHIVE	60
 TRAINING QUESTIONS AND ANSWERS	 61
 FREQUENTLY ASKED QUESTIONS ABOUT CHECK 21 ACT (FAQs)	 61
POWERPOINT TRAINING PROGRAM	66

REFERENCES OF APPLICABLE RULES AND REGULATIONS	67
FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC)	67
FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)	67
FEDERAL RESERVE BANK (FED)	68
NATIONAL CREDIT UNION ADMINISTRATION (NCUA)	68
THE OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)	69
OFFICE OF THRIFT SUPERVISION (OTS)	69
STATE DEPARTMENTS OF BANKING	70
RISK MANAGEMENT OF REMOTE DEPOSIT CAPTURE	71
QUICK REFERENCE	71
RISK MANAGEMENT: RISK ASSESSMENT	72
OCC INTERPRETIVE LETTER #1036	72
GRAMM, LEACH, BLILEY ACT (GLBA) 501(B)	73
RISK MANAGEMENT: MITIGATION AND CONTROLS	73
FFIEC BANK SECRECY ACT/ANTI-MONEY LAUNDERING (BSA/AML) EXAMINATION MANUAL	73
FFIEC IT EXAMINATION HANDBOOKS	74
WHAT IS THE INFOBASE?	74
WHAT CAN BE FOUND ON THE INFOBASE?	74
INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS – SMALL-ENTITY COMPLIANCE GUIDE	75
FEDERAL RESERVE AND TREASURY DEPARTMENT ANNOUNCE FINAL RULE ON MERCHANT BANKING ACTIVITIES	75
FDIC LAW, REGULATIONS, RELATED ACT	75
NCUA RECORD RETENTION	75
INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION	76
LEGAL AND COMPLIANCE RISKS	76
CHECK CLEARING FOR THE 21ST CENTURY ACT (CHECK 21 ACT)	76
FFIEC CHECK 21 INFOBASE	76
AUTOMATED CLEARING HOUSE (ACH) CHECK CONVERSION	76
REGULATION E	76
USA PATRIOT ACT	77
INTERAGENCY GUIDANCE ON AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT	77
UNITING AND STRENGTHEN AMERICA’S APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM	78
RISK MANAGEMENT: MEASURING AND MONITORING	78
SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS	78

LEGAL REFERENCE DISCLAIMER

This “*2013 Corporate and Consumer Rules and Regulations Toolkit®*” (Training Manual) was developed to provide assistance to financial institutions and their customers that use Remote Deposit Capture. The Training Manual was developed based on research from individuals, companies and state and federal agencies. Every effort was made to identify all materials quoted with appropriate footnotes that identify the original authors, agencies and companies that originally publishing the material.

The sale and provision of this Training Manual by any company representative or person does not constitute endorsement of, or by, T. Houston Technology Group, a Georgia Corporation, and no part of the Training Manual is meant to be construed as legal advice or any other form of business recommendation to any person, financial institution, or user of the Training Manual concerning the products and services described herein.

As with all legal matters and documents, a reader or user should consult with a qualified attorney on all matters discussed in this Training Manual before taking any related action, using any form or document discussed, referenced or published.

WHAT'S NEW IN REMOTE DEPOSIT CAPTURE?

Remote Deposit Capture (“RDC”) continues to make great strides in adoption rates, system features and benefits. Because of the flexible architecture of the systems, it also poses a dark side—the opportunity for terrorists and drug dealers to transfer money in support of illegal activities. Hence, the purpose of this book. We will publish an updated version each year to apprise users of the legal and technology changes in Remote Deposit Capture so you can update your program to comply with new or changed rules or laws—or ensure that your company takes advantage of new features.

If we miss a change that you are aware of, please let me know at Thouston@thouston.com or call at 281-756-0409.

The following are changes that you will see in the coming months:

1. Remote Capture has taken a large step into the world of Smart Phones. Mobile Deposit Capture has made an explosive entry into the financial world and adoption is explosive. Take picture of the front and back of a check and transmit it to the Financial Institution does the rest. Fast, simple and secure.
2. Policies, procedures and training materials for compliance of the new Remote Deposit Capture guidelines.
3. Narratives, examples and descriptions of the major components of Remote Deposit Capture are provided to build a solid foundation on which to build training programs for the successful use of the technology that continues to deliver significant benefits to millions of users.
4. Federal and State Regulators and Examiners are now reviewing whether the audit requirement of RDC customers is being conducted internally and by third-party companies. This is not new for 2013, but enforcement is being seen across the financial industry. This is a great opportunity for your company or agency to learn and understand the basic Risk Management practices used and perfected by financial institutions for 3 decades.
5. New guidelines for all financial institutions, “Supplement to Authentication in an Internet Banking Environment,”¹ require stringent security changes in financial institutions effecting their customers were implemented January 1, 2013. The purpose of the new guidelines is to help reign in cyber-crooks and hackers that are targeting American financial institutions and their customers almost daily. The Internet is allowing fraudsters from all over the world the opportunity to find weaknesses in the firewalls and electronic infrastructures of businesses in America and attack them with almost total immunity. A great aid to all Financial Institutions are resources brought to bear by The Texas Department of Banking, which has done a great job educating financial institutions and their customers with a website designed specifically for Account Takeover Education.²

¹ <http://www.fdic.gov/news/news/press/2011/pr11111a.pdf> (accessed 1/25/13)

² Best Practices, Texas Department of Banking, www.ectf.dob.texas.gov (accessed 1-25-13)

INSTRUCTIONS FOR USING “2013 REMOTE DEPOSIT CAPTURE RULES & TRAINING GUIDE”

T. Houston Technology Group has documented and published this training manual to assist financial institutions, businesses and consumers in understanding the rules and regulations necessary for the safe and legal operation of Remote Deposit Capture.

We encourage you to read the book, update the policies provided in the Remote Deposit Capture Toolkit, obtain approval from management or Board of Directors, conduct training classes and implement your program. The resounding comment we hear repeatedly is, “I wish this technology was developed sooner.”

This Book is intended to be used with the other documents in the Remote Deposit Capture Toolkit. It makes references to several chapters. If you do not have the Toolkit, contact your RDC provider and ask them to provide you with an updated copy, or call us at 281-756-0409.

We have developed the Rules & Training book to flow in a logical way, but use the Table of Contents if you have specific topics in mind.

Annually, we will publish a new edition of this guide for Remote Deposit Capture and recommend that you update your materials and training program accordingly. Additionally, we will appraise participating financial institutions of any changes or situations that require immediate attention in order for them to notify you or your company.

REMOTE DEPOSIT CAPTURE WORKPROGRAM

Texas Department of Banking

Overview³

It is important to understand how federal and state regulators view a product or technology. This narrative describes the view of the Texas Department of Banking. This narrative is excerpted from their Audit Program, which is also available at: <http://www.banking.state.tx.us/examproc/bnkexampro.htm> (accessed July 10, 2013). We recommend that each area of your financial institution read their section of the RDC Audit to gain an insight on how to prepare and the questions you will be asked during the audit.

“Remote Deposit Capture (RDC), a deposit transaction delivery system, allows a financial institution to receive digital information from deposit documents captured at remote locations. These locations may be the financial institution’s branches, ATMs, domestic and foreign correspondents or locations owned or controlled by commercial or retail customers of the financial institution. In practice, the vast majority of banks are only offering the RDC application to commercial customers. In substance, RDC is similar to traditional deposit delivery systems at financial institutions; however, it enables customers of financial institutions to deposit items electronically from remote locations. Generally, branch capture of deposits presents less risk, because internal controls have already been put in place. As a result, these procedures address the necessary elements of an RDC risk management process in an electronic environment, focusing on RDC deployed at a customer location.

Smaller financial institutions have normally outsourced the RDC function to a vendor, where larger institutions will sometimes have this application in-house. Appropriate vendor management practices should include adequate review of the RDC vendor. RDC allows financial institution customers to deposit items electronically from remote locations. The primary RDC delivery method is the Internet, whether to the bank or the vendor. The RDC product is similar to Internet banking. The customer uses the Internet to sign on and then scans the deposit items. If the deposit balances, it is transmitted to the institution/vendor for processing. If the deposit does not balance then either the customer or the vendor will make corrections, prior to processing.

The FFIEC has issued guidance for examiners in FIL-4-2009 (for non-member banks) and SR 09-2 (for member banks). Additional guidance can be found in the FFIEC issued I.T. booklets on Safeguarding of Customer Information guidelines.”

³ Narrative: <https://www.dob.texas.gov/examproc/it-15-rdc.pdf> (accessed July 10, 2013)

CHECK 21 ACT AND REMOTE DEPOSIT CAPTURE BASICS

Why Check 21 Act?

Remote Deposit Capture (RDC) is as large and innovative as any new technology since the advent of PC Banking. Two words in the “*Check Clearing for the 21st Century Act* (“*Check 21 Act*”),” “foster innovation,” may have sparked the idea of creating a system that allows businesses and consumers to capture checks and create deposits from their offices and homes. The result is a change in the payment system that revolutionizes making a deposit.



Immediately after 9/11, U.S. item processing was nearly paralyzed because the airlines that normally transport checks among large cities were grounded. Millions of checks were stored in cargo bays of airplanes sitting idly for two days on tarmacs.

The trucking industry was unable to take up the slack of delivering checks because they were forced into service hauling and staging critical supplies in preparation for another

attack. The impact of not being able to deliver checks had a devastating effect on many businesses, especially small businesses that rely on daily revenue for their existence.

During the aftermath of 9/11, congress established a task force to study the impact on the financial system and determined that the time had come to implement advanced technology that would insulate and allow the national check processing system to function during any future crisis. The Check 21 Act was passed on October 28, 2003 and went into effect one year later. Check 21 Act (Check 21) was designed to improve check-clearing efficiency, lessen the need for paper checks, and continue clearing operations during a disaster. The mandate was clear—reinvent the national item processing system with advanced Internet technology. The innovation that grew out of the rebuilding process was Remote Deposit Capture at the customer’s location; the legal framework of Check 21 provided check image vendors with the direction they needed to enhance their check image systems for Internet image exchange.

Check 21 Act Created Framework

To avoid resistance in the financial community, congress elected to make participation in Check 21 voluntary, which means a financial institution can send and receive check images or only receive images

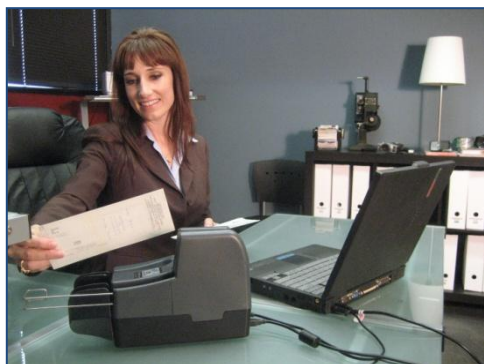
The **Check Clearing for the 21st Century Act** (or **Check 21 Act**) is a United States federal law, Pub. L. 108-100, enacted into law October 28, 2003 by the 108th Congress. It took effect one year later, on October 28, 2004. The law allows the recipient of a paper check to create a digital version, thereby eliminating the need for further handling of the physical document. Source: Wikipedia

and Substitute Checks. A financial institution cannot refuse to accept Substitute Checks described later in the “About Checks” chapter. Substitute Check are also called Image Replacement Document (IRD) and are images converted back to paper in a special format as needed. In all cases, the financial institution that sends an image to a non-Check 21 financial institution must bear the cost for processing the image into a Substitute Check format and delivery.

Remote Deposit Capture System

RDC systems are typically small, powerful desktop systems that include a workstation, desktop scanner, laser printer, and software to capture checks and transform them into an electronic deposit that is

transmitted to the pre-arranged financial institution.⁴ The scanners range in speeds from 8 documents per minute (DPM) to 180 DPM. As the checks move through the scanner, an internal digital camera takes high-resolution images of the front and back of each check and records them to a hard-drive. Another



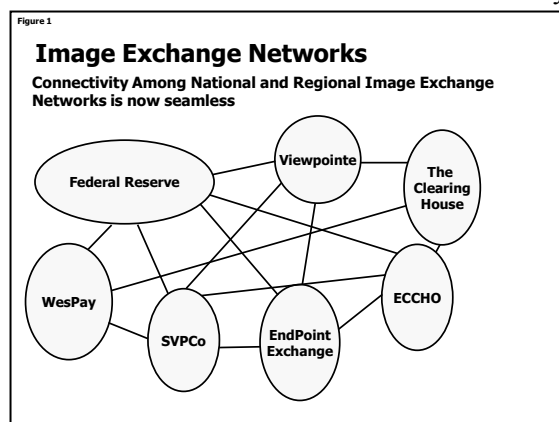
device in the scanner is a special reader that identifies the magnetic ink characters (MICR) located at the bottom of each check, records them, and links them to the check image. The MICR line contains routing information for the financial institution the check is drawn on. Throughout the capture, correction, and balancing process, the system keeps a running total⁵ of the checks to assist the operator in balancing the deposit. After balancing, the checks are transmitted via the Internet to the business or consumer's financial institution, or service bureau, as part of the collection process. After all

checks are scanned, deposit total balanced and transmitted—the original checks should be stored immediately in a safe location.

When received by the financial institution, a computerized process separates the checks drawn on the customer's financial institution and electronically forwards the other checks, called transit items, to their paying bank.

Overview of the Value of Check 21

Financial institutions have the option of creating, processing, and exchanging digital images of checks rather than actually transporting the original paper check to the Maker's institution for payment. U.S. consumers and businesses write billions of checks each month, which are then processed for deposit and collection. This requires large staffs, high-speed machines, supplies and expensive transportation to move checks from the financial institution where they are first deposited to the checkwriter's financial



institution. Although this process has been streamlined several times to make it work as smoothly as possible, it is still one of the most expensive services for financial institutions to provide.

Image Exchange Networks

Check 21 did not define specific warranty and indemnity requirements of image exchange among financial institutions. Therefore, an agreement to exchange images must be executed by each financial institution that participates in image exchange.

⁴ Only items drawn on U.S. financial institutions qualify for Check 21

⁵ Requires Courtesy Amount Recognition/Legal Amount Recognition modules

Across the U.S., multiple Clearing Agents (authorized companies to process check images) have formed a latticework of high-speed, encrypted networks to send and receive check images constantly for financial institutions. Advanced technology, similar to systems used in ATM networks tracks each item from the time it enters the network until the time it is delivered to its final destination. Each financial institution that participates in Check 21 processing is a member of a participating network that manages the routing of millions of images each day.

The connectivity ensures that a check image is transmitted via the fastest, most efficient route for payment. If for any reason a check cannot be processed via the Image Exchange network, it is printed in Substitute Check format and transported by courier to the paying bank.

In today's systems, most financial institutions use "batch processing" for image exchange. This means the financial institutions hold the checks until the end of the business day and transmit all of them at the same time. This method is used because Check 21 is relatively new compared to other services, such as ATM processing. Long-term, Check 21 processors will send individual checks at the time they are received. The design of the networks and opportunity to mitigate fraud seems to indicate that transmissions will eventually parallel ATM processing, which is usually real-time mode.

Debits = Credits

Each night Clearing Agents in the Check 21 exchange network settle the millions of checks sent and received using "settlement accounts" at the Federal Reserve Bank or a correspondent bank. This method of bookkeeping enables each financial institution to determine their starting and ending settlement balance for each business day. Similar to businesses and consumers, financial institutions have to balance their accounts—but they are required to reconcile settlement accounts on a daily basis.

Return Items

As each business day begins, checks from the previous day that could not post at the paying bank begin the return process. The most common reasons that checks are returned are insufficient funds, closed accounts, and stop pay orders.⁶ The Federal Reserve Bank provides an electronic image return service that obsoletes the paper-check return system that financial institutions have used for decades. This fast turnaround on bad checks will allow the financial institution to alert RDC customers that a check is being returned so they can begin the collection process sooner.

Remote Deposit Capture was Started in Mexico

RDC began in Mexico by check image vendor AFS⁷ and Wachovia Bank. A little strange considering that RDC is only allowed for checks drawn on U.S. financial institutions. However, Wachovia had several large customers doing business in Mexico who overnighted their deposits to the U.S. for next-day credit. After both companies conducted legal research and their attorneys found no reasons in Check 21 not to use RDC, the RDC technology process began.

6 Ezine Articles, Collecting Bad Checks - Returned Check Collection Options for Individuals and Businesses, <http://ezinearticles.com/?id=731292>

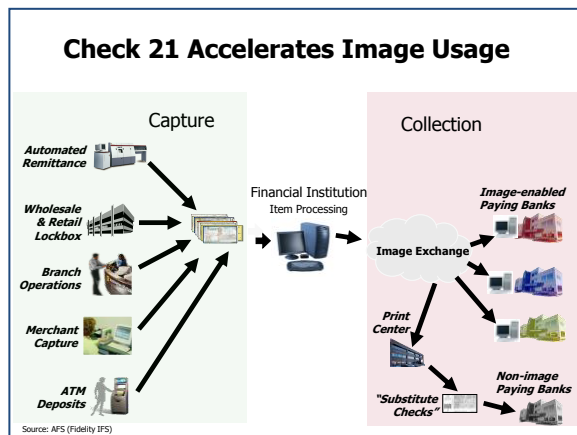
7 Amy Harlow, Metavante Image Solutions (now Fidelity IFS)

Remote Deposit Capture Solves Transportation Problem

During the decade preceding Check 21, retaining reliable and reasonably priced courier service was a major problem. High gas prices and labor costs prevented many courier companies from retaining drivers and caused them to overload pickups on critical routes. In turn, this meant the checks from financial institutions could arrive late at the processing center and they would not receive same-day credit for their deposit of customer checks. The significance of the courier problem was an issue that most financial institutions tackled each time they opened a new branch; how to get the checks and deposits to the central item processing center?

Solving the courier problem was a constant battle for branch managers and RDC immediately got their attention. Research found customers that used RDC believed the benefits were attainable, desktop check scanners were reliable and affordable, Internet usage was fast and secure, and customer employees strongly endorsed its use because of the convenience and elimination of driving to the financial institution to make the deposit. RDC was a solution to the courier problem that plagued almost every financial institution in the United States.

For more than two decades, financial institutions and customers have used check images for statement rendering, but until The Act, images did not have the legal status to replace original paper checks.



Earlier capture systems were analog-based and sorters (large scanners) used cameras that recorded images on microfilm. Before the images could be used for research—the film had to be processed, which could easily take 1-2 days. Since microfilm was chemical-based, the quality of the images began to deteriorate immediately after the film was processed. Check image systems now digitally capture and store checks.

When stored on a computer using this technique, the pristine quality of the image is maintained indefinitely. Printing a check image will produce the same quality

as the original—regardless of how long it has been stored. Since check images are typically stored on a hard drive, access is fast for any authorized workstation from the RDC or Online Banking system.

Check 21 Accelerates Image Usage

After technologists learned how to harness the power of check image and Check 21, it paved the way for significant upgrades to older products. Before Check 21, only large financial institutions and service bureaus could afford Remittance Processing systems. Post Check 21, prices for these products plummeted 75% - 80% for complete and robust systems. Smaller financial institutions and customers have implemented systems that provide advanced functionality and reduce operating costs.

Remittance Processing

Remittance Processing is a great example of how the convergence of small image scanners and software developed for large volume processing can be scaled down to the desktop for small businesses.

Remittance processing is a service that includes capturing, balancing, posting, and depositing of a customer coupon and payment check. It significantly reduces the manual labor involved in processing remittance documents and check payments. Phone bills are a good example; the customer normally receives a bill for the service and returns the bill with a check payment. Next, the Remittance system is used to read the remittance document and check payment to ensure the check amount is correct for the payment. If all of the information is correct and the payment is on time, a record is created from the remittance document to update the customer's account with the phone company. The check image created as part of the process is included in a file transmitted to the financial institution for processing into the phone company's account. Although the process seems simple, it usually involves dealing with numerous customer issues, such as partial payments, wrong remittance documents, late payment charges not being added to payment, etc. However, it was not payment issues that kept financial institutions from providing the service—but the cost.

After Check 21 was enacted—several vendors reengineered their RDC systems to include a module for Remittance processing, and the price plummeted more than 75% for a complete and robust system. Remittance Processing benefits are no longer just for large institutions and service bureaus—any business that receives and processes remittance coupons and payments could benefit from today's systems.

Image Enabled ATMs

An image is an image—whether it is created in a business office or an ATM. Several companies now offer ATMs that accept checks and create a check image that is routed to the paying bank almost the same way a check is routed from a business office or a consumer's scanner. Many of the same advantages are provided to the customers that use these ATMs; better availability of funds that are a result of electronic collection and earlier notification if a deposited check is drawn on an account that is closed or has insufficient funds. The public has become aware that the era of check float is rapidly coming to an end.

Check 21 Reduces Float Time

Most Americans are used to the convenience and speed of Internet-based E-mail and many businesses would probably say they are dependent on it. However, because of Internet speed in delivering checks from bank-to-bank, check float⁸ is disappearing.

Checks captured using RDC in Nashville, Tennessee, can be securely transmitted to a paying financial institution in San Francisco, California, within minutes, thereby eliminating float time. In the past, it would normally take 2-3 days to collect the check using a combination of airline and ground transportation. The current environment and technology has reduced collection time dramatically and system enhancements will someday allow a check to be processed much like an ATM transaction—which is immediate. Although advanced check technology may change the banking habits of companies and consumers, it will also provide the benefit of notifying customers sooner when they have received and deposited bad checks.

⁸ The time between issuing a check and having the funds deducted from a deposit account.

Timely Product for “Self-Service Society”

During the past decade, the U.S. has seen the “Self-Service Society” become a reality with RDC fitting in seamlessly. Gas stations, grocery stores, fast food restaurants and now financial institutions are providing service that is more convenient than traditional methods.

Customers can now select the time that is convenient for them to make checking account deposits and not be driven by the clock. Plus, not having to drop off the deposit on the way home could mean more family time.

Benefits of Remote Deposit Capture

Improved Availability of Funds

**Remote
Check
Capture**



**Simple
Safe
Convenient**

**Scan the checks – push the button.
Deposit made electronically.**

The benefits of Remote Deposit Capture are numerous and measurable:

- Cost for Making Deposit is Less
- Convenience – Make Deposit at Your Desk and Eliminate Driving to Bank
- Extended Cutoff Times
- Better Availability of Funds
- Greatly Improved Research
- Eliminate Interrupting Employees to Make Deposit

Call Shawn Smith today and let us show you how making a deposit with Merchant Check Capture is fast and simple.
Call today: (713) 568-2056

For a CEO, few things are allowed to come before managing the company's cash flow. Projecting and managing the cash positions are a CEO's commitment to fiscal soundness. As important, is the use of information technology to maximize the return on funds and avoid unnecessary labor costs.

Many times, getting checks deposited on Wednesday means payroll can be funded on Friday. Improving cash flow with Remote Check Capture is easy for many companies. The larger the company, the more common it is to see checks missing the 2:00PM cutoff

while they make their way through a maze of internal company processes and are handled by many different employees before being collected and deposited. In some companies, the mail may not be distributed until the afternoon, which guarantees next-day deposit processing. RDC mitigates these problems with multiple deposit transmissions throughout the day and some institutions have changed their deposit deadlines to a later time.

Now, RDC can give time back to the customer because it eliminates the drive time to make the deposit.

Cost Reduction for Making Deposits

One of the obvious benefits from RDC is the cost reduction for making deposits. Having an employee drive to the financial institution is expensive when you consider mileage and salary cost. Even harder to quantify is the cost of interrupting an employee's normal duties. Several studies have found that RDC takes about half the time of an employee travelling to the financial institution to make the deposits and you can schedule the RDC at the least disruptive time.



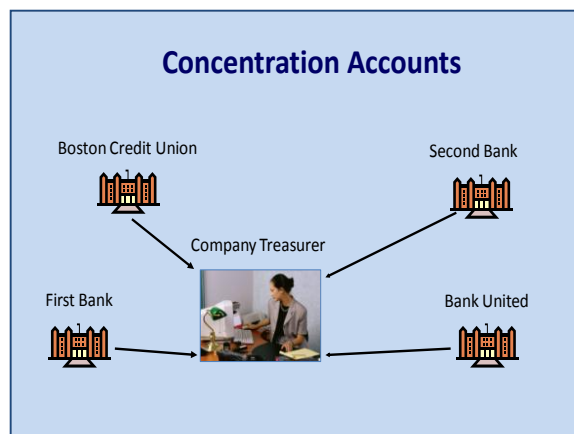
Employee morale may improve because one of the most dreaded deposit scenarios is avoided—missing the deadline by 5-minutes and having to explain why the deposit will not be credited until the next day.

Eliminate Hazard of Driving in Bad Weather

No one hates the ice and snow of winter more than the employee assigned to drive to the financial institution to make the deposit. No matter how careful and experienced the driver, the trip is necessary but dangerous. Insurance companies should be apprised when businesses implement RDC because it reduces the risk of having a weather-related accident and the associated liability.

Cash Concentration of Funds

Businesses need to concentrate funds for various reasons, but primarily for paying normal expenses or making investments. It can be difficult for the corporate treasurer to determine available balances when funds are kept in multiple financial institutions. Consolidating funds in a master account makes it easier for the treasurer to determine investable funds, which is critical for projecting cash flow and may allow earlier investment of funds.



For companies with outlying branches or offices, the use of RDC as a funds concentration tool can be very effective.

RDC allows companies to scan checks from any office and deposit them directly into the operating account at the customer's primary financial institution.

Using RDC to concentrate funds is usually less expensive than maintaining deposit accounts at distant institutions. Most financial institutions have minimum collected balances that have to be maintained or an account is service charged. Additionally, concentrating

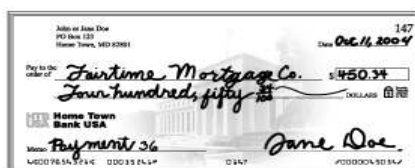
funds may raise the collected balance at the primary institution and, through Account Analysis, reduce or eliminate the monthly service charge.

Before RDC, ACH was the preferred concentration system, but it normally took two business days to move funds from different institutions to the primary account. With RDC, the funds are usually available⁹ the morning after the transmission is completed.

Wire transfers can be used to concentrate funds when the need for funds is urgent, but the charges for each wire are typically between \$15.00 to \$20.00. Wire charges may vary significantly among institutions.

Regardless of how it is accomplished, funds concentration is another important self-service product.

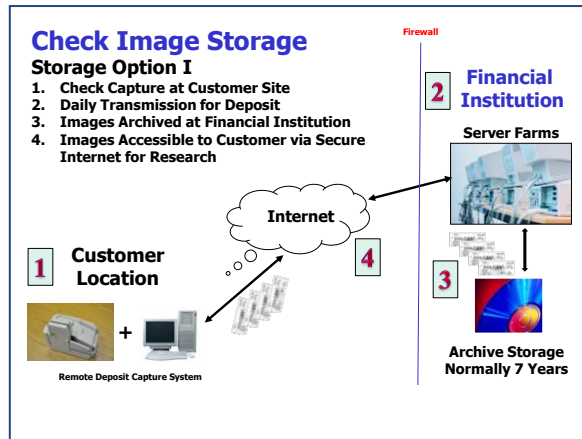
Fast Research



Although the approach for storing check images is vendor-dependent, all systems provide a fast method for researching checks processed by businesses and consumers. Check images are not located by information contained in the actual image, but instead the search program looks for text data that is linked to the

⁹ Funds availability is subject to the financial institution's availability schedule.

image. In the example on the left, the arrow is pointing to the searchable information on the check: serial number, routing information, and amount of the check. When the check is captured by the scanner, the bottom line, called the MICR line, is captured by a special feature in the scanner and stores the information and the image link. Although you cannot see the data, it stays with the image throughout its



life. The related data is stored in a database that is indexed allowing immediate access to the check image. This search method is critical when you consider that over time a financial institution, or its service bureau, will store millions of check images and customer access must be fast and efficient.

Check Image Archive Models

There are several configurations and variations for archiving check images, but the following two examples are typical of how financial institutions keep the check images available for fast and secure access.

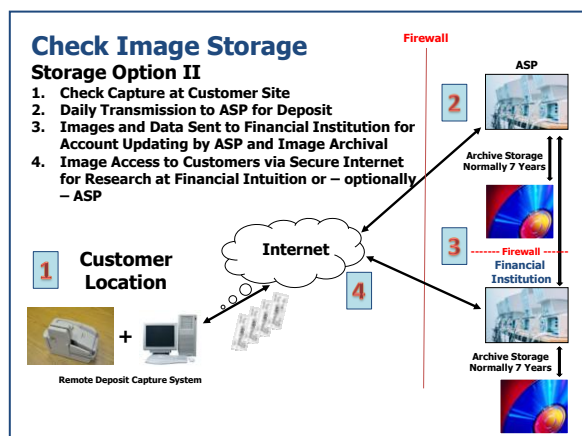
As shown in Option I, the check image and related data is captured at the customer's location and forwarded to the financial institution for deposit. After processing, the financial institution transfers the images to a storage archive, which is normally kept for 7 years. As a digital image, the quality does not deteriorate over time, but maintains the same high resolution as the original image.

When a customer needs to see a check, it is accessible via RDC or Online Banking System, depending on the configuration and parameters set by the financial institution.

In Option II, the financial institution uses an application service provider (ASP), which is a specialized service bureau, to provide RDC to their businesses and consumer customers.

ASP services are a viable alternative to in-house systems because their resource sharing lowers their per institution cost for processing. For example, an ASP may have a dozen financial institutions and their customers sharing a server farm instead of an individual financial institution building and maintaining a server farm for only their customers. Another advantage is software maintenance.

Each time an ASP customer initiates a RDC session—they always get the most current version of the software. Programmers at the ASP can update and test the software until it is ready for use by customers



and when they put it in production all customers will immediately begin using the same version. This avoids having customers on different versions of the software, which can mean different commands and procedures. ASPs are becoming common in the financial industry, as well as other industries, because of these and other benefits.

This option also shows that a customer may retrieve archived images from the financial institution or the ASP, depending on the configuration implemented by the financial institution. Years of experience in the

item processing industry has taught vendors and financial institution managers that you can never have too many backups.

Electronic Security

The old adage, “A chain is only as strong as its weakest link,” is certainly applicable to the U.S. financial system. Every financial institution and their RDC customers have an important responsibility to keep their link secure.

The primary regulators of financial institutions conduct an annual Information Technology (I.T.) audit to ensure that networks and Internet systems are developed and operated in the most secure manner possible. With RDC, security audit requirements extend beyond the financial institution to their business and consumer customers who use the service.

“Information security is the process by which an organization protects and secures systems, media, and facilities that process and maintain information vital to its operations. On a broad scale, the financial institution industry has a primary role in protecting the nation’s financial services infrastructure. The security of the industry’s systems and information is essential to its safety and soundness and to the privacy of customer financial information.”¹⁰

To ensure the security of customer information—advanced and proven security systems and procedures should be implemented before RDC is installed and operational. The security guidelines published by the FFIEC require layered security, *“The FFIEC agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.”*

Authentication

“Authentication is the verification of identity by a system based on the presentation of unique credentials to that system. The unique credentials are in the form of something the user knows, something the user has, or something the user is. Those forms exist as shared secrets, tokens, or biometrics. More than one form can be used in any authentication process.”¹¹



Passwords Are Not Enough

For years, passwords were the linchpin for security, but the simplicity of their design made them easy targets for hackers. According to the Computer Emergency Response Team¹² (CERT), 80% of the security attacks they investigate are password related. The vulnerabilities of password-based solutions stem from a combination of the following:

- Employees aren’t perfect and should not be relied upon to maintain a process that is highly rules-based
- “Job-related” processes compete for attention
- Certain insiders or outsiders are intentionally looking for ways to compromise the solution¹³

¹⁰ FFIEC Information Security Audit Handbook, page 4

¹¹ FFIEC Information Security Audit Handbook, page 21

¹² CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University

¹³ Source: DigitalPersona.com

Single Factor Authentication

Single factor authentication (SFA) is typically defined as a unique identification code (ID) and password. Although common in non-financial systems, the use of simple codes and passwords, such as Susie, Spot or July4—were vulnerable to hackers that used specialized programs to guess the codes and obtain unauthorized access to information. To strengthen the financial system, institutions installed multi-factor authentication (MFA) systems, which significantly strengthened authentication.

Multi-factor Authentication

Multi-factor authentication (MFA) is a security system in which more than one form of authentication is used to validate a user's login.

MFA can be as simple as adding a pass phrase or selecting a picture from a collection electronically presented to you when the account was opened, which is a third secret element.

Security is significantly improved when MFA is supported by an automatic lockout after three incorrect login attempts. Additional authentication methods, such as biometric verification and smart cards are also used being used to strengthen MFA.

No longer “James Bond” technology, the use of Biometrics fingerprints is becoming widely used across the financial industry. This technology is more expensive than relying on secret codes, but the effectiveness is undisputed and it is now available as standard equipment on many new laptop computers. This is especially important since laptops can easily be lost or stolen.

Dangerous Systems are Available on the Internet

Key Loggers, such as the one below, are legal to buy and use—when it is for the right reason. However,

The advertisement for WebWatcher Computer Monitoring Software features a woman standing next to a computer. The text highlights its capabilities as a key logger, claiming to 'Capture every Keystroke - GUARANTEED' and offering a 'LIMITED TIME 40% OFF' discount. It lists features such as Email Recording, Instant Message Recording, Keystroke Logging, Website Monitoring & Blocking, Monitor from Anywhere, Content Filtering, Take Screenshots, and Completely Invisible. The ad also mentions it is 'Always Rated the #1 Monitoring & Control Software' and has been featured on CNN, HeadlineNews, Newsweek, CBS NEWS, and abcNEWS. A 'BUY NOW' button is prominently displayed.

when these programs are secretly installed on an employee's workstation they can gather sensitive and confidential information about the employee, company, and other types of non-public information.

The key logger program can record every keystroke that is typed into the computer: IDs, Passwords, account numbers, websites, etc. These programs can be set to E-mail the collected information to any offsite location with Internet access, which means anywhere in the world.

Unparalleled Invisibility Technology

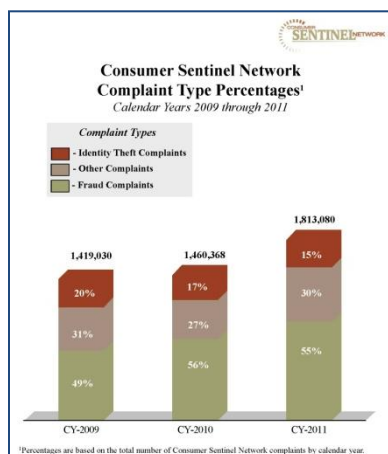
WebWatcher doesn't appear ANYWHERE. No one will ever know it's there.

Once the information is obtained by a hacker, it can allow unauthorized access to confidential company

information, online administrative accounts, accounts at financial institutions, etc. The list is as long as the authorized access of the employee that is victimized. For less than \$100.00, a company or consumer can be compromised and never know it.

Hacking and ID Theft are Major Issues

If the emphasis on security seems overblown, consider the statistics behind it. Each year, millions of Americans report identity theft, which results in unauthorized use of debit cards, credit cards, accounts at financial institutions, etc. It is not uncommon for an identity to be stolen and used to purchase a house or car. The regulatory inter-agencies, local, and state law enforcement have opened a new chapter in identity theft because of the magnitude of the problem nationwide. Leading the battle is the Federal Trade Commission, which has a well-established reporting network and provides an abundance of resources for protecting your family and business from identity theft.



Consumer Sentinel Network

Federal Trade Commission (FTC)

The Consumer Sentinel Network¹⁴ (CSN) is a secure online database of millions of consumer complaints available only to law enforcement. In addition to storing complaints to the FTC, the CSN also includes complaints filed with the Internet Crime Complaint Center, Better Business Bureaus, Canada's Phone Busters, the U.S. Postal Inspection Service, the Identity Theft Assistance Center, and the National Fraud Information Center, among others.

Law enforcement agencies, whether they are down the street, across

¹⁴ <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf>

the nation, or around the world, can use information in the database to enhance and coordinate investigations. Upgraded features make searching complaints more efficient. Begun in 1997, to collect fraud and identity theft complaints, the CSN now has more than 7 million complaints, including those about credit reports, debt collection, mortgages, and lending, among other subjects. The Sentinel graph is a comparison from the first CSN annual report that analyzes the central database. Between January and December 2011, CSN received more than 1.8 million consumer complaints, which it sorted into 30 categories.

Identity theft was the number one complaint category in the CSN for calendar year 2011 with 15% of the overall complaints, followed by Debt Collection (10%); Prizes, Sweepstakes and Lotteries (6%); Shop-at-Home and Catalog Sales (5%); Banks and Lenders (5%); Internet Services (5%); Auto Related Complaints (4%); Impostor Scams (4%); Telephone and Mobile Services (4%); and Advance-Fee Loans and Credit Protection/Repair (3%).

- For military consumers, Identity Theft was the number one complaint category in the CSN, followed by Debt
- Collection at number two. Mortgage Foreclosure Relief and Debt Management ranked as the fourth highest category for military members, in contrast to thirteenth highest for the population as a whole.

Fraud

- A total of 990,242 CSN 2011 complaints were fraud-related. Consumers reported paying over \$1.5 billion in those fraud complaints; the median amount paid was \$537. Sixty-eight percent of the consumers who reported a fraud-related complaint also reported an amount paid.
- Sixty percent of all fraud-related complaints reported the method of initial contact. Of those complaints, 43% said email, while another 13% said an Internet website. Only 7% of those consumers reported mail as the initial point of contact.
- Colorado is the state with the highest per capita rate of reported fraud and other types of complaints, followed by Delaware and Maryland.

Identity Theft

- Government documents/benefits fraud (27%) was the most common form of reported identity theft, followed by credit card fraud (14%), phone or utilities fraud (13%), and bank fraud (9%). Other significant categories of identity theft reported by victims were employment fraud (8%) and loan fraud (3%).
- Complaints about government documents/benefits fraud increased 11 percentage points since calendar year 2009; identity theft-related credit card fraud complaints, on the other hand, declined 3 percentage points since calendar year 2009.
- Forty-five percent of identity theft complainants reported whether they contacted law enforcement. Of those victims, 70% notified a police department. Fifty-seven percent indicated a report was taken.

- Florida is the state with the highest per capita rate of reported identity theft complaints, followed by Georgia and California.

Improving Traditional Security Systems

For companies and consumers that cannot upgrade their systems to advanced technology, simple but stronger techniques can be applied to existing security. When you create a password, think about a dictionary, because hackers have easy access to “Cracker” programs that use all of the words in a standard dictionary and thousands of “most commonly used passwords” in their attempt to breach systems.

What Not to Use

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

What to Use

- Do use a password with mixed-case alphabetic characters.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation.
- Do use a password that you can remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Requirement to Periodically Change Passwords

Passwords should be changed periodically to combat unauthorized use. This especially holds true for employees who leave the company. Ensure that your system can easily handle password changes.

Multiple Security Levels

There are several levels of security provided in most RDC systems, and, except for supervisors, you need to differentiate access on an “as needed” basis. Make sure the system does not have a “one size fits all” approach.

Encrypted Transmissions

As required by federal and state regulators, each transmission between the customer and financial institution, or its agent, must be encrypted. On television, this is usually shown as rows of “0” and “1.” In reality, it is much more complex than audiences would find interesting, but the important point is encryption is an integral part of all RDC system transmissions. “In general, encryption functions by taking data and a variable, called a “key,” and processing those items through a fixed algorithm to create

the encrypted text. The strength of the encrypted text is determined by the entropy, or degree of uncertainty, in the key and the algorithm.”¹⁵

Check Capture Equipment Trends

Paradigm Shift to Decentralization

During the past decade, there has been a measurable change in the item processing paradigm, from centralization to decentralization. Previously we discussed the difficulty in retaining reliable and affordable couriers for financial institutions. Customers did their part by driving to the institution and making the deposit, but many institutions used service bureaus and had to courier the checks to a central location. This critical issue was not missed by check image vendors who developed feature-rich desktop scanners that were typically more technologically advanced than the large sorters and normally created personnel savings for the business users. Why courier a check when you can use RDC and transmit it in minutes? An additional benefit for many financial institutions was the savings in courier drive-time, which was passed on to the customers in the form of later deposit deadlines.

1980 Monetary Control Act

This little known law, “Requires the Federal Reserve to set prices to recover, over the long run, its total operating costs of providing payment services.”¹⁶ Since Check 21 did not mandate financial institutions to use check image, the Fed found itself in a precarious situation of offering both paper check and digital check services. In response to the 1980 Monetary Control Act, the Fed has frequently raised prices on expensive paper-based services and lowered them on electronic services. The result is an unintended “*prod*” to paper-based financial institutions to move to efficient digital technology.

Desktop Scanners Rule

Small, feature-rich, and easy to operate, RDC scanners have a strong footing in tens-of-thousands of businesses. During the transition to desktop scanners, vendors were tasked with making “user friendly”



more than a tag line each time a check image vendor implemented a system. Implementation by first generation businesses and consumers has gone smoother than most pundits expected.

Low Cost-High Tech Scanners

These scanners are small, but packed with high-tech circuitry and programs that were designed and built based on proven technology. Many of the same companies that built the big sorters for the past 40 years are now building desktop scanners. However, a few new vendors are using their flatbed scanner and imaging experience to create scalable and reliable

check scanners that compete favorably with those produced by the seasoned veterans.

¹⁵ FFIEC IT Examination Handbook, page 50

¹⁶ Source: <http://www.fdic.gov/regulations/laws/rules/8000-2200.html>, 8000 - Miscellaneous Statutes and Regulations{ {4-30-86 p.8537} }, DEPOSITORY INSTITUTIONS DEREGULATION AND MONETARY CONTROL ACT OF 1980

The aggressive competition has caused scanner prices to fall more than 30% during the past two years and sales are booming.

Starting at prices that are less than most businesses pay for personal computers, the growth path for desktop scanners is clear and affordable. Some vendors have an initial scanner price that is intended to prevent sticker shock, but are scalable to meet the highest volumes. For example, a business with an entry-level, eight (8) documents per minute (DPM) scanner, has an option to buy another scanner at the same speed, which doubles the capture rate, or step-up to one that matches the actual check volume and keep the original scanner as a backup. Perhaps the best part is the system and commands remain the same and only the scanner changes.

Desktop Check Scanners come in all sizes with a plethora of optional features:

Check Processing Speed

- Capture Speed – 8, 30, 70, 120, 180 DPM

Check Input

- Hand Feed
- Hopper Support – up to 100 checks

Image Capture Mode

- Simplex: Capture Only Front or Back of Check per Pass
- Duplex: Captures Front and Back of Check per Pass

Resolution

- Bitonal (black/white)
- Gray level (256 gray shades)
- Color (24-bit, RGB)

Image Renditions

- 300 dpi Color
- 200, 240 dpi gray level or bitonal
- 100, 120 dpi gray level

Image Compression Standards

- CCITT Group 4 (bitonal images)
- JPEG Baseline (gray level images)
- Uncompressed 24-bit, RGB pixel color (color images)

Endorsement

- Front Franker
 - Franking roller with fixed message
- Rear Endorser
 - One (1) to four (4) line endorsement, 10 characters per inch
 - Two (2) vertical endorsement, 10 characters per inch
 - Two (2) vertical endorsement locations, manually selected by operator allows eight (8) single-line vertical endorsement locations

CHECK 21 ACT AND REMOTE DEPOSIT CAPTURE WARRANTIES AND INDEMNITIES

Definitions for Clarification of Certain Topics

“Truncate means to remove the original check from the forward collection or return process and to send, in lieu of the original check, either a substitute check or, by agreement, information relating to the original check. Truncation does not include removal of a Substitute Check from the check collection or return process.”¹⁷

“Converting Bank” means the financial institution that converts an original check into a check image or Substitute Check.

“Indemnity means security against hurt, loss, or damage; or exemption from incurred penalties or liabilities.”¹⁸

“Reconverting Bank” means “(A) the bank that creates a substitute check; or (B) if a substitute check is created by a person other than a bank, the first bank that transfers or presents such substitute check.”¹⁹

Network Foundation is Based on Warranties and Indemnities

The successful growth of a national image exchange network requires clear and concise rules for the orderly operation and legal protection of the participants. From the day the Check 21 Act went into effect, the growth has been significant and technologists agree that nothing on the radar will slow it down. The days of having employees manually inspect paper checks has faded into history. Financial institutions and their customers must adapt to an electronic banking environment where hardware, software, rules, and laws replace many of the manual processes used for decades by financial institutions.

The ACH network and Check 21 network seem to be in juxtapositions, but, actually, ACH has a 30-year head start.

Good News and Bad News

As reported by the FDIC²⁰, fraud occurs less in RDC than the general population. What should be obvious kudos for financial institutions and their customers has delayed a legal necessity—very few lawsuits.

Lawsuits may seem like an odd necessity for stability in a technology, but, until the ragged edges are trimmed away in courts of law, we only see the theoretical side of the legal intent. Lawsuits, and their inevitable appeals, result in arguments among attorneys and scholars that refine how technology will eventually operate and what safeguards are necessary to protect financial institutions and their customers.

For example, the ACH transaction, “Accounts Receivable Conversion (ARC),” had at one point the requirement to destroy a check within 14-days of conversion. Initially this made perfect sense to the rule makers that were trying to keep a check from being represented. However, after a particularly contentious lawsuit, the requirement was dropped in favor of having the original check available for forensic inspection. Another large area that needs clarification is image quality.

¹⁷ Federal Reserve System, 12 CFR Part 229, DDD. 229.2(ddd) Truncate, page 84

¹⁸ Merriam-Webster 11 Collegiate Dictionary

¹⁹ Check 21 Act, Definitions (3) (B) (15)

²⁰ FDIC Supervisory Insights Summer 2009, page 21

Check 21 Act does not clearly define what an acceptable check image looks like; therefore, we must rely on agreements among participants to establish the legal foundation for image acceptability. Image Quality Assurance (IQA) programs and their developers do an excellent job of technically addressing the issues, but, until we have legal precedence²¹, we cannot have settled law.

Warranties²²

For Check 21 to operate as intended the legal foundation, which is based on warranty and indemnification, must provide assurance to the participants that the Substitute Checks and images they receive meet the requirements defined by the Act. Therefore, each participant in the chain must warrant and indemnify the next participant in the chain (Transferee) for the Substitute Checks and images (by Agreement) they transfer to them.

The Image Exchange Network is handling billions of image items annually and it is unlikely that the success of Check 21 could have been realized without the warranty and indemnity protection of Check 21, related laws, and clearinghouse rules.

“In business and legal transactions, a warranty is an assurance by one party to the other party that certain facts or conditions are true or will happen; the other party is permitted to rely on that assurance and seek some type of remedy if it is not true or followed.”²³

“When a financial institution sends a check for collection or presentment, it makes warranties and takes on liabilities with respect to that check under Regulation CC, state law (the Uniform Commercial Code), and, if it sends the check to a Federal Reserve Bank, Regulation J. In addition, the financial institution may take on other responsibilities with respect to the check as agreed to between the participating institutions by contract or clearinghouse rules.”²⁴

We are all used to warranties; we rely on them when problems occur with a new car, cell phone, computer, appliances, etc.

“Financial institutions that participate in Check 21 also make warranties that the check images and Substitute Checks they create or transfer are not duplicates and “the information accurately represents all of the information on the front and back of the original check as of the time the original check was truncated.”²⁵

Duties for All Financial Institutions

“All banks that transfer, present, or return a substitute check for consideration thereby make the substitute check warranties and indemnities described in Regulation CC. However, in the vast majority of cases, liability for the warranties and indemnity ultimately will flow back to the reconverting bank.

²¹ In common law legal systems, a precedent or authority is a legal case establishing a principle or rule that a court or other judicial body utilizes when deciding subsequent cases with similar issues or facts. Source: Wikipedia.org, (Accessed July 16, 2011)

²² <http://www.ffiec.gov/exam/check21/faq.htm>, (Accessed July 16, 2011)

²³ <http://en.wikipedia.org/wiki/Warranty>(Accessed July 16, 2011)

²⁴ FFIEC Risk Management of Remote Deposit Capture, page 3, footnote 6

²⁵ Check 21 Act, Section 6 (d) (1)

Because a substitute check must be suitable for automated processing in the same manner as an original check, a bank that receives a substitute check will not need to change its equipment and will need to make only minor processing changes if it returns a substitute check.”²⁶

Indemnities

“Banks that transfer, present, or return a substitute check, or a paper or electronic representation of a substitute check, also indemnify subsequent parties against losses due to the receipt of a substitute check in place of the original check. A valid indemnity claim can only be made by a recipient of a substitute check. As with the warranties, the indemnities also flow back to the first reconverting bank.”²⁷

Although the above federal requirement addresses financial institutions and the Check 21, the financial institutions are required by FFIEC guidelines²⁸ to impose the same, or similar, requirements of their customers

Duties for All Customers

The FFIEC guidelines mandate that the customer’s RDC agreement include requirements that hold the customer accountable for ensuring that items are not resubmitted and the image quality is acceptable.

Example of a RDC Customer Agreement

Responsibility for Warranties.

- (a) Company agrees and warrants (regardless of whether the warrantee receives the substitute check or another paper or electronic form of the substitute check or original check) that no depository financial institution, drawee, drawer, or endorser will receive presentment or return of the substitute check, the original check, or a copy or other paper or electronic version of the substitute check or original check such that the financial institution, drawee, drawer, or endorser will be asked to make a payment based on a check that the financial institution, drawee, drawer, or endorser has already paid.
- (b) Company agrees that it will maintain policies and procedures to ensure that the check images captured, front and back of each check, and transmitted to financial institution are high resolution and readable, in accordance with requirements defined by Check 21 Act, Section 4 (B)(1).

Although the requirements may seem stringent, they are necessary for the protection of all financial institutions and their customers. With millions of participants in RDC transmissions, each customer must carefully operate their system and ensure that the quality of images produced is acceptable. The Remote Deposit Capture Procedures Chapter provides instructions on how these requirements may be met.

²⁶ <http://www.ffiec.gov/exam/check21>, Duties for all banks, page 8,(Accessed July 16, 2009)

²⁷ <http://www.ffiec.gov/exam/check21>, Indemnity, page 6, (Accessed July 16, 2009)

²⁸ FFIEC Risk Assessment for Remote Deposit Capture, Contracts and Agreements, page 6

ABOUT CHECKS

Not all of the items that tellers routinely handle are candidates to Check 21 Act and Remote Deposit Capture. After careful evaluation of all item types—the final version of Check 21 allows as many items as possible without creating issues in the payment system.

Qualified Items

All checks, including cashier's checks, payroll checks, personal checks and business checks are subject to Check 21 Act. This list represents the preponderance of all item processing transactions. When these items are converted into Substitute Checks, they do not lose their qualification for electronic delivery and presentment.

Qualified Items

- Any check may be truncated in either the forward or return presentment stream
- A properly constructed substitute check (aka IRD) may be used instead of the original check *if the sending institution so desires*
- Images may be used instead of the original *only by agreement between the sending and receiving institution*
- A receiving institution need not accept images, but it has no say whatsoever in whether the paper it receives is an original check or a substitute check

Non-Qualified Items

- Non-U.S. Items
- Items in Carriers
- U.S. Savings Bonds
- Checks Without MICR Line

Non-Qualified Items

As you can see in the chart on the left, the restrictions on items represent a small number, but each could cause issues when transmitted electronically and presented to the Paying Bank.

The Check 21 Act was written specifically for U.S. financial institutions and “non-U.S. Items” cannot be captured and deposited into a U.S. financial institution. However, Remote Deposit Capture systems can and are used in locations around the world to capture and transmit checks for deposit drawn on U.S. financial institutions.

In the earlier chapter, we discussed the first installation of Remote Deposit Capture, which was installed in Mexico for U.S. companies.

Foreign checks cannot be processed using RDC because of the myriad of different laws and rules in banking systems.

Later in this chapter, we discuss the reasons why

check carriers must not be used in RDC. Although many customers remember receiving the yellow envelopes with a partially mutilated check inside, the requirements in the electronic world no longer allow these documents.

U.S. Savings Bonds

Savings bonds are not checks and therefore are not subject to Check 21.²⁹ These transactions must be placed in a separate envelope and “special handled” by the Federal Reserve Bank. “Bonds are a low-risk, liquid savings product. While you own them, they earn interest and protect you from inflation. You may purchase Bonds via TreasuryDirect, at most local financial institutions or through payroll deduction.

²⁹ www.aba.com/ABAEF/checksarechanging.htm (Accessed July 23, 2009)

As a Treasury Direct account holder, you can purchase, manage, and redeem Bonds directly from your Web browser.”³⁰

Substitute Checks

The conversion of paper checks to electronic check images dramatically reduced the cost of handling checks and created the opportunity for widespread adoption of Remote Deposit Check Capture (RDC). RDC is arguably the most important financial technology of this decade and will have a lasting impact on how customers make deposits.

Federal Reserve Defines Substitute Check

“A substitute check is a paper copy of the front and back of the original check. A substitute check is slightly larger than a standard personal check so that it can contain a picture of your original check. A substitute check must be printed in accordance with very specific standards so that the substitute check can be used in the same way as the original check. If you receive a substitute check that appears to have a problem, such as it contains a bad picture of your original check, contact your bank.”³¹

Legality of a Substitute Check

A substitute check is legally the same as the original check if it accurately represents the information on the original check and includes the following statement: “This is a legal copy of your check. You can use it the same way you would use the original check.”

If you receive a substitute check that is the same as the original check and you suffer a loss related to the substitute check, Check 21 Act provides you with a special procedure for obtaining a refund. However, even if you have received and deposited a bogus check, you are under a time limit to discover the bad check and return it to the financial institution (refer to your Deposit Agreement for specifics).

As shown in the following chart, Substitute Checks have peaked and are declining as more financial institutions deploy Check 21 and image-based item processing. Substitute Checks (IRDs) were managed to low volumes because they cost 4-5 times more to create, deliver, and settle than a check image.

Front View of a Substitute Check



³⁰ http://www.treasurydirect.gov/indiv/products/prod_ibonds_glance.htm

³¹ <http://www.federalreserve.gov/paymentsystems/truncation/faqs2.htm>

Back View of a Substitute Check



Types and Purposes of Images

Several years ago, many financial institutions converted to check image statements and stopped returning the original paper checks in statement, but instead provided a “statement sheet” of images that represented the checks and deposits processed that month. Normally, there were 12 images to a page, and the image size and number of images per page is adjustable to accommodate customers that are visually impaired. Financial institutions can actually print the images 3 to a page, which increases the image size and makes reading the information on each check much easier.

The pictures on the image statement represent an original check or a substitute check. Whether the consumer or business receives an original check, a substitute check, an image statement, or a line item on his or her account statement, check law and federal regulations protect consumers and businesses against erroneous and unauthorized check payments. In addition, Check 21 Act provides a special refund procedure, called “Expedited Recredit,” for victims of check fraud.

Under Check 21 Act, financial institutions are required to provide a Check 21 disclosure to their consumer customers who receive canceled checks with their monthly statements. The disclosure describes consumer rights regarding substitute checks. The disclosure must also be provided when a consumer requests an original check or copy of a check and receives a substitute check. In addition, the financial institution must provide this disclosure if a check the consumer has deposited is returned unpaid to the consumer in the form of a substitute check.

Check Endorsements

Because of the tremendous number of checks processed each day, most financial institutions will examine endorsements and signatures only on high-dollar items.

If you receive and deposit a fraudulent check or a check drawn on an account with insufficient funds, it will normally be returned from the paying bank and charged back to your account. Your financial institution is required to provide “Ordinary Care”³² for check processing, but it is the responsibility of the business and consumer to know their checkwriters and verify their identification.

³² <http://www.law.cornell.edu/ucc/3/3-103.html>, .C.C. - ARTICLE 3 - NEGOTIABLE INSTRUMENTS § 3-103(a) (7)

In most cases, if you use a desktop check scanner, it may allow printing one or more lines of endorsement, such as “***This Check Has Been Electronically Captured by First National Bank of Anytown, Texas.***”

Usually, the wording of the print line can be modified by the financial institution providing the Remote Deposit Capture system.

Supplemental Check Information

When a check is imaged using Remote Deposit Capture additional information is also captured, but not necessarily printed or displayed until needed. For example, attached to a check image is data that identifies the “Origination ABA, Process Date, File Creation Time, Destination FRB Prefix, Destination Institution Name, etc.”³³ The information is used by computer programs for routing the check image to a financial institution, printing Substitute Checks and returning checks that may be drawn on insufficient or closed accounts. These electronic endorsements are an important part of the endorsement process and allow seamless electronic movement of check images.

Rules for Exchanging Images Among Financial Institutions

The Check 21 Act did not mandate participation of financial institutions, but provided the framework necessary to create and operate a national image exchange. The Electronic Check Clearing House Organization (ECCHO) “was created in 1990 by banks as a cooperative venture to encourage the use of electronics to enhance the check collection system. ECCHO’s primary activities can be divided among three functions: 1) rules development and maintenance, 2) industry education and 3) industry advocacy.”³⁴

ECCHO not only writes the rules for image exchange, but provides central management of agreements among financial institutions that want to participate in image exchange but do not want to sign and maintain thousands of agreements with other financial institutions. Members of ECCHO can customize their participation agreement from multiple options and only provide the services they deem appropriate. For example, a financial institution can elect to send images but not receive them.

Another critical feature of the ECCHO agreement is warranties³⁵ provided to the receiving institutions from senders: i) Member has complied with ECCHO Rules, ii) Electronic Image accurately reflects the Related Physical Check, iii) Electronic Image is an acceptable quality, iv) Electronic Image is not a duplicate of another Electronic Image. Although these warranties may seem basic to the process of image exchange, they are not provided as such in the Check 21 Act.

ECCHO’s requirements for endorsements are clear, “As paper checks are converted to electronic documents and back to paper IRDs, the endorsement chain must be maintained.”³⁶ Another form of endorsement is required in the form of a “Presentment Notice” which contains the MICR line (Routing Information to the Paying Institution).

Additionally, the Supplemental Check Information described above is also attached to each check image. The combination of the endorsements provide fast and accurate information when one of the billions of checks processed annually require research.

³³ Source: Federal Reserve Bank, Migration to the DSTU X9.37-2003 standard

³⁴ The Electronic Check Clearing House Organization, ECCHO CONNECT, Overview

³⁵ The Electronic Check Clearing House Organization, Rules Summary

³⁶ The Electronic Check Clearing House Organization, Check 21, Endorsements

Customers Cannot Require Original Paper Check

Because of the legal status given to Substitute Checks, customers that have previously received their paper checks back in their statements can no longer be guaranteed that they will continue to receive them. Instead, they may receive Substitute Checks from other financial institutions. The financial institution of first deposit may use a check image system and convert the check into an image for forward collection to the paying financial institution. At that point, the paying institution only has the image and not the original paper check. For statement preparation of checks that have been converted to Substitute Checks, the customer must accept them in lieu of the original paper check. It is important to note that all of the information on the original check, front and back, is captured and available for research and printing.

Check Carriers

DO NOT USE CHECK CARRIERS WITHOUT PERMISSION FROM YOUR FINANCIAL INSTITUTION.

Check Carriers, sometimes called document carriers, have been used in traditional item processing for several decades. Their purpose is to provide an envelope for transporting mutilated checks through the item processing system to the paying bank. Prior to check imaging, this approach worked well, but the construction of the envelope wreaks havoc on check images. The envelope front is plastic and is not transparent, but translucent. The back is typically 24# paper. This means that you lose the ability to image capture the endorsement and handling information that is normally stamped on the back of a check. It also

Example - Check Carrier



means that a financial institution cannot create a qualified Substitute Check from the image. Also see “Substitute Checks” section above.

Eliminating the ability to create a Substitute Check negates one of the primary benefits of the Check 21 Act—creating a legally equivalent document that replaces the original check.

The Federal Reserve Banks prohibit carriers for high-speed electronic cash letters. “The Fed will no longer accept items in carrier documents in Forward 21 image cash letters and Return Item cash letters. These items must be forwarded by the depositing bank to the paying bank as a manual collection item. This includes carriers containing photocopies in lieu, notices in lieu of return and foreign or mutilated items. In order for Banks to offer products that fully enable the opportunities of the Check 21 Act ground-breaking law, it is important that these items are not included in high-speed processing cash letters. Industry experience shows that image quality for these types of items often doesn't meet a high standard for readability, which prevents conversion to substitute checks.”³⁷

The expense for handling check carriers begins at the financial institution. Per Federal Reserve Bank Rules, “The following kinds of items may be sent to the Fed only in a specifically identified cash letter containing only items of the kinds listed here: any item in a carrier envelope.”³⁸ To separate checks in carrier envelopes means manually locating the check carriers, creating a separate group of checks,

³⁷ Federal Reserve Banks, Operating Circular No. 3, Collection of Cash Items and Returned Checks, Effective July 15, 2008

³⁸ Federal Reserve Bank, Operating Circular 3, Section 6

preparing a list using an adding machine or capturing the items using a special run, and transporting the checks to the Federal Reserve Bank for forward collection.

The Federal Reserve Bank also sent a letter to all financial institutions in mid-2008 reminding them that check carrier items cannot be included in high-speed image cash letters. This includes check image transmissions where the original checks remain at the business or consumer's location, e.g., Remote Deposit Capture customers.

Image Quality Assurance (IQA)

"Beauty is in the eyes of the beholder" Margaret Wolfe Hungerford.

As many people, and especially technologists and programmers, know defining beauty or the quality of an image is a daunting task. For financial institutions, having a computer program that defines acceptable image quality is essential because of the billions of check images processed that must be analyzed to ensure acceptable quality. The image of a check will be seen by the paying institutions' customers on their deposit statement, and they will assume it is their institution that created a high resolution or poor quality image. However, a more critical reason may be the legal issues involved with Image Quality.

Check 21 Protections

Two Warranties

- Legal Equivalence Warranty
- No Duplicate Debit Warranty

Indemnity Against Losses Due to Substitute Check

Expedited Recredit Process

Source: FFIEC Check 21 Presentation

When a paper check is converted into an image, the process is defined as "truncation,"³⁹ and the paper check is removed from the payment system and replaced with a check image and routing information taken from the original check's MICR line. Thereafter, the image and related data are used to complete the payment of the original check.

When an image or Substitute Check is presented for payment, both must accurately represent the Original Check.⁴⁰ If it does not, it negates the transfer indemnity provided by the Check 21 Act and the Paying Bank

may dishonor the presentment and request the original check or a check image with acceptable quality. This would mean having the check rescanned and represented, which would be very time-consuming and costly. However, if the Bank cannot obtain the original item and cannot reproduce an acceptable image and related data from its archive, the truncating Bank is legally responsible for the liability created.

In the case of a financial institution's Customer that originally scanned the check, the institution may require, by Agreement, that the Customer produce the Original Check or an acceptable check image. Either way, the burden for resolving the issues lies with the Truncating Bank.

³⁹ Check 21 Act, Section 3, (18)

⁴⁰ Check 21 Act, Section 4, (b) (1)

Check 21 Act Does Not Define Quality

Check 21 Act does not provide comprehensive guidance for truncating checks, but provides the legal framework that allows financial institutions to execute agreements with other institutions, or authorized agents of other institutions, for processing check images. These agreements require financial institutions to provide certain warranties and indemnities when exchanging check images for collection or return.

Since the quality of a truncated check (image) is not covered in the Check 21 Act, the agreement among participating institutions would provide a warranty (guarantee) that the check image accurately represents the information on the original check and would require that the resolution of the image is usable, or readable by a person.

The complexity of defining image quality is obvious in the construction of the law, but the law clearly states that a “Substitute Document” must “accurately represent all of the information” which defines a de facto image quality standard.

High Resolution Image



As billions of checks are truncated, the reliance on computer systems to test and alert financial institutions of an issue becomes critical.

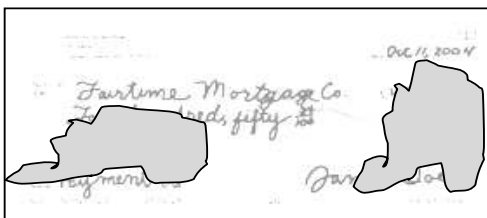
When you look at the first example, it is easy to see the product of a good system, hardware and software, and the resulting image. Everything on the front can be easily read or printed. The back of the check was not shown, as it

would not necessarily add anything to the topic. Either the image is good or it is not.

Throughout the image exchange process, and even later at the Paying Bank, computer programs will be the first line of defense against fraud and that requires high resolution images to work properly.

For example, many financial institutions use programs to compare signatures on checks to identify potential fraud through forgery. The programs use advanced technology to compare the signature of the

Poor Image Quality



last three checks processed and determine if the handwriting is from the same person. If a difference is detected, the system flags the check for additional manual review. If the image quality is poor/unacceptable it negates the opportunity to immediately spot fraud and take appropriate actions.

As you can see from the second example, the image quality is extremely poor and most likely, if detected, the Paying Bank will request a replacement of the original paper check or an acceptable image of the original check. They will also be reluctant to send an image that looks like this one to their customers. This also shows clearly that even though these are only examples, in the “real world” these types of issues and differences in image quality occur thousands of times each business day.

It is important to remember that the transition to image exchange is a voluntary epoch in item processing and the changes have to be made slowly and carefully.

IQA is vendor dependent and the Check 21 Act does not specify how to measure image quality. Once again, financial institutions turned to the private sector to define quality and how to implement measurements that serve the purpose intended and remain affordable.

Metric / Defect	
Undersize Image	Horizontal Streaks in Image
Folded or Torn Document Corners	Below Minimum Compressed Image Size
Folded or Torn Document Edges	Above Maximum Compressed Image Size
Document Framing Error	Excessive "Spot Noise" in Image
Excessive Document Skew	Front-Rear Image
Oversize Image	Dimension/Feature Mismatch
Piggyback Documents	Carbon Strip Detected
Image Too Light	Image Out of Focus
Image Too Dark	

Source: The Financial Services Technology Consortium (FSTC)

Standardizing the specifications of check images also avoids a key issue common with early check image systems that were proprietary. When a financial institution changed core vendors, which typically meant changing check image vendors, the image formats were often incompatible. That meant that the institution had to pay extra to have their images converted into the new format. Check images have evolved significantly over the past decade and will continue to do so with the guidance of groups, such as

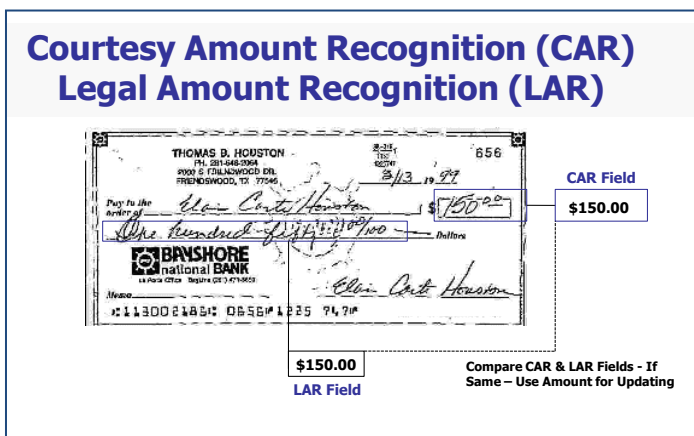
the FSTC. This group is part of the American National Standards Institute (ANSI) and continues to research, collaborate, and publish techniques that enhance the quality of check images.

Partial Measurements

Part of the work published by the FSTC Group is the Metric/Defect Chart above. Although the actual number of tests have increased, this chart provides a basic description of what a computer program would test an image for to determine if the quality is adequate.

Courtesy Amount Recognition (CAR) and Legal Amount Recognition (LAR)

When a checkwriter writes a check to make a purchase payment, etc., the information is handwritten or computer printed. To process the check—the amount field must be encoded for the intended amount. The process of entering the amount is performed by a proof operator or using a Courtesy Amount Recognition (CAR) and Legal Amount Recognition (LAR) program.



On the surface, the process seems fairly simple operation, read the check image in a specific location and translate the information into data that can be processed by the computer, but a number of factors create challenges for the conversions.

Lift Technology Cleans Up Check

If you ever wondered why the little “puppy dogs” that are printed on your checks do not show up on your image statements, it’s because “lift technology” erases them to

keep check image data sizes to a minimum. Long used in image technology, lift technology is expert at identifying superfluous data, such as the pictures that make checks more interesting.

Although the “I Love Quarter Horses” with a picture of a beautiful horse is nice, it significantly increases the image size and creates clutter that affects CAR/LAR conversions. Lift technology is fine-tuned to avoid erasing important information, such as names and address, amount and payee information. It also avoids the MICR line at the bottom of a check that is required to properly route a check to customer’s financial institution. It creates a “clean area” around the fields necessary to allow CAR/LAR to convert a high percentage of amount information into data without operator intervention.

Roles of CAR/LAR

Although CAR and LAR fields are located in specific locations on a check, the presentment of writing or computer printing is usually different and requires unique processing for each area of the check. CAR technology has been used successfully for more than a decade and its purpose is to electronically convert numeric information into data.

The CAR engine starts the process by searching an area that would normally contain the \$ symbol, which signals where the program should start looking for numeric information. The \$ is fairly standard on most checks and represent the easier part of the process. Since the amount field only contains numeric information 0-9, processing is restricted to these characters. The CAR engine is normally tuned to perform conversion of a digit based on a “confidence level” established by the user. The higher the confidence level is set, the higher the accuracy of the digits converted. This results in more digit rejects. Digit rejects are normally shown on a balancing screen as * in the position of the rejected digit.

The LAR engine may be used in combination with the CAR process and together produce a much higher number of successfully converted image amounts into editable data. As compared to CAR processing, LAR encounters greater conversion issues due to the handwriting practices of checkwriters.

Handwriting varies from near-calligraphy to almost unreadable scratching style and may include all alphabetic characters, a combination of letters and number and special characters such as / or – as part of the legal amount. The goal of the LAR engine is to recognize as many letters and words as possible, which increases the overall success rate of the combined process.

For example, CAR may accurately convert 65% of all numbers with a high confidence factor, 10% at a slightly lower confidence factor and 25% with low or no confidence (reject digit) factor. When combined with LAR, digits that may be borderline with the CAR engine may be validated with LAR, boost the success rate to 75%-80% and lower the questionable digits in the next two tiers. Depending on the volume of checks processed, lowering the corrections may represent a significant savings in personnel time.

CAR/LAR Accuracy

CAR/LAR engines are tuned using parameters controlled by the user and do not present new risk. Checks captured through Remote Deposit Capture should always balance to a control document. When a capture run is out of balance, the system will display the digits on checks it cannot read but it will not force-balance the deposit. The operator will view the check image and make the necessary corrections. The confidence levels of CAR/LAR are controlled by the user and can be set to require the same accuracy as a proof operator.

Check Image Compression

Check images are large and complex pieces of information for computers to handle. The workstation and scanner translates each piece of an image into a digital code and stores it in memory. The typical size of an uncompressed, bi-tonal check image can run 720,000 bits or 90,000 bytes just for the front of a 3" x 6" personal check. (A byte equals eight bits for most computer systems, and a bit is the smallest piece of information a computer handles, a single "either/or" kind of code character, like the binary digits 0 or 1).

Too bulky as they first exist, check images have to be compressed into a smaller size and format for normal usage. The most commonly used format is Tagged Image File Format (TIFF), which is controlled under a patent held by Adobe Systems.

TIFF images are bit-mapped pictures. This means that originally smooth and continuous pictures have been changed into bits of computer binary code. When these bit-mapped images are displayed again, they appear as a series of tiny dots, much like the dots you can sometimes see in newspaper photographs. TIFF images are common in many computer applications, and hundreds of vendors provide software to handle them. In fact, most fax machines and scanners create TIFF images.

Vendor May Store Multiple Copies of Image

The initial check image may be compressed to about 20,000 bytes, including both the front and the back of the check. Compare that to 1,480,000 bytes for an uncompressed image of a check (front and back) in terms of storage space needed! The "rule of thumb" for printing images is the bigger the better. These large formats produce a high quality that is required for printing images on customer statements.

However, the larger image file create processing issues when you consider the volumes of checks processed each day. To facilitate transmission needs and meet Federal Reserve requirements, images are formatted and compressed to a low, but usable level of bitonal (black and white), TIFF. "The TIFF validation will align Federal Reserve Check 21 deposit requirements with ASC X9.100-181-2007, the Specification for TIFF Image Format for Image Exchange."⁴¹ In this announcement, the Fed not only reported that they would use the industry standard TIFF image, but also test images for quality.

The new standard includes:

- Image Format–TIFF 6.0
- Image Compression–CCITT G4, 200 or 240 DPI resolution, Black and White (Bitonal)
- Character Code–ASCII or EBCDIC except for binary image data
- Quality Check–Checks will be tested for length, height, validity, missing or torn corners, document skew, image brightness, and compressed image size.

AUTOMATED CLEARING HOUSE (ACH)

The ACH network was started by a group of California bankers in 1972⁴² as a system for handling small-dollar items and was hailed as the beginning of the "checkless society." Americans were told to, "Kiss you checks goodbye," because they would be gone by the end of the '70s.

⁴¹ Press Release, Federal Reserve Banks Announce Check 21 Validation Changes in Test Environment, April 30, 2009

⁴² NACHA, "The History of NACHA-The Electronic Payments Association"

Although the early adopters and proponents of ACH had the right idea, they misjudged the reluctance of Americans to give up their checkbooks. According to the Federal Reserve Bank (Fed), check volumes grew steadily until about 1995 and then started a slow decline. In 2011, U.S. check volume is expected to drop to around be about 17.9 billion⁴³. While check volumes are declining, ACH transactions continue to increase. In 2008, ACH transactions grew 7.07% to 14,960,689,587.⁴⁴

ACH and Remote Deposit Capture Technology Compete

RDC and the Internet have changed bank technology forever. Financial institutions of all sizes are offering systems that deliver on their benefits' promise, and half of the RDC systems being sold have an integrated ACH module.

Although ACH has a long and successful history as a transaction system, trying to explain the differences between it and RDC is a daunting task for even the most experienced technologist.

ACH and Check 21 Act Technology and Laws/Rules are Different

Starting with the technology used and ending with the rules that govern each transaction, both systems can handle a check all the way through the payment system.

Check “Conversion” vs. “Truncation”

Conversion

- Use an electronic scanner to read certain information from a paper check or Substitute Check and create (Conversion) an electronic record based on that information for collection of the funds represented by the paper Check
- Examples: ARC, POP, and BOC
- Governance: Primarily NACHA Rules, Electronic Funds Transfer (EFT), Federal Financial Institutions Examination Council (FFIEC), and Agencies and Uniform Commercial Code (UCC)
- Transaction is no longer a “Check” governed by Check Law during transmission
- Image is not part of the clearing process

Truncation

- Use an electronic scanner to create an image (picture) of a paper Check or Substitute Check and electronically transmit the image and related data (Account Number, Routing Number and Auxiliary Field, Serial Number and Amount) for collection of the funds represented by the paper check
- Stop the paper check early in the collection process, forward collecting as an image or substitute check
- Governance: Primarily Check 21 Act, Federal Financial Institutions Examination Council (FFIEC) and Agencies, Uniform Commercial Code (UCC), and ECCHO Rules
- Image or Substitute Check have same legal status as original check – when created properly

ACH Transactions for Remote Deposit Capture

It seems ironic that the 2013 ACH Rules⁴⁵ book for businesses is several hundred pages of detail rules and regulations about a system, that when it is reduced to the base level, is a “debit” and a “credit.” To be

⁴³ <http://www.reuters.com/article/pressRelease/idUS205794+24-Jul-2008+BW20080724>

⁴⁴ NACHA Press Release, April 12, 2013, “Overall ACH Volume Exceeds 20.2 Billion in 2011,” <https://www.nacha.org/node/1130> (accessed June 10, 2013)

⁴⁵ 2013 ACH Rules, Corporate Edition, The National Automated Clearing House Association

more concise—the debit=credit. However, the management of NACHA has for years responded to the needs of U.S. businesses and citizens and continually enhanced ACH transactions to meet those needs.

Each time NACHA has introduced a new transaction—the acceptance has been immediate as they have always addressed issues that allow businesses and consumers to reduce their cost and improve collection time.

The three transactions used for Remote Capture:

- Point of Purchase (POP)
Available September 15, 2000
Used for checks written during check-out, check voided and returned to checkwriter and converted to ACH transaction⁴⁶
- Accounts Receivable Conversion (ARC)
Available March 15, 2002
Mailed checks or drop box for bill payment and convert to ACH transaction
- Back Office Conversion (BOC)
Available March 16, 2007
Collect checks during cashier's shift or business day and convert to ACH transaction

RDC & ACH

Many RDC systems have been designed to capture checks into ACH and Check 21 formats for collections. Although the two processes handle checks differently, in many cases the features and benefits overlap and create confusion about which one to use.

ACH transactions were a solid success long before RDC because it was a cheaper, faster, and better collection method than paper checks. When the U.S. Postal Services is used to deliver bills and payments, the collection process is dependent on factors that range from traffic to employee attendance. Electronic delivery avoids most of these issues and provides a dependable and predictable delivery schedule.

Today, QuickBooks™⁴⁷ can generate an invoice for a product, or service rendered, and deliver it by email within a few minutes of pressing the Send key. The same invoice can be approved, paid, and archived on the same day it was sent. By eliminating the multiple people that normally handle paper payments and checks, the funds are usually available to the Biller days sooner.

Whether RDC or ACH, the users are the winners; electronic transactions are faster, cheaper and safer than paper transactions.

⁴⁶ Subject to NACHA Rules

⁴⁷ Number 1 Accounting System in the U.S., owned by Intuit

INTERNAL CONTROLS

The Remote Deposit Capture Policy provided in this manual is for illustration purposes only. It is not meant to be used without review and approval from your management or a qualified attorney.

Remote Deposit Capture provides significant benefits, but also presents risks that must be defined and addressed by the financial institution that is providing this service and the customers that use it. The requirements and risks vary by customers and factors such as size, location, check volume, and technology environment. The skills of the users and support personnel determine the controls necessary for the safe and productive operation of the system.

The following policy is intended as a guide for creating and using known processes and safeguards for electronic systems. A significantly expanded version is used by all U.S. financial institutions. We encourage you to review the Policy and update it to meet all of your risk management requirements.

Contact the financial institution that provides your system if you have any questions and let us know at Thouston@thouston.com of topics or changes that we should include in the 2013 update.

Reader's Note: Purpose of this section.

This section is intended to provide the reader with a sample Policy document. You may change the document, but a similar Policy is required by the federal examiners to be adopted as part of your Official Company Records. Additionally, your Financial Institution is required by regulations to ensure all of their customers have this or a similar Policy.

Remote Deposit Capture Operations and Risk Management Policy

Statement of Purpose

The Board of Directors (**Optional - Senior Management**) of **CUSTOMER NAME** (Company) has identified the need to establish, document, and distribute the Company's Remote Deposit Capture (RDC) System and Risk Management Policy. These guidelines will provide the parameters for the following components:

- Risk Management
- Privacy of Information
- Document and Resource Management
- Human Resource Management
- Software Maintenance
- Levels of Access to Information
- Information Technology Security Safeguards
- Unauthorized Access to Information Notification
- Vendor Oversight
- Alternate Deposit Plan
- Employee Training
- Authority and Review

The Board views RDC as an essential financial service to control costs and eliminate the risk of requiring an employee drive to the financial institution to make deposits.

While communicating the Board's philosophy about goals of safety, soundness, profitability and responsiveness to our business needs, this Policy is not intended to replace the experience and sound judgment of executive officers and managers.

Background

In most areas of business, technology and the Internet are changing business paradigms that have been in place for decades. The financial industry is also changing dramatically due to the Check Clearing for the 21st Century Act (or Check 21). This law provided the framework for financial institutions to exchange check images instead of paper checks. The results are new products and services that transmit encrypted checks to their paying financial institution at Internet speed.

RDC is a financial service that allows a Customer to remotely scan checks, automatically convert them into industry standard check images, and electronically transmit them through an Image Exchange Network (IEN) to **YOUR FINANCIAL INSTITUTION** for deposit.

The system is comprised of a desktop computer, small check scanner, printer, and application software. The application software operates the scanner, converts the paper checks into electronic images, verifies the quality of each check image or allows individual viewing of each image, and ensures the total of the checks balance to a pre-determined amount. Before transmission to the financial institution, the system creates a "Virtual Deposit Ticket," eliminating

the need for the paper document. The system also creates archive storage for the check images, which provides advanced research capabilities.

When **YOUR FINANCIAL INSTITUTION** receives the electronic deposit, operational procedures ensure the checks are processed into Company's account and an electronic receipt is generated for printing by Company.

The emergence of Remote Deposit Capture is a prime example of how financial managers are taking advantage of proven technology to enhance the Customers' banking experience and decrease their related expenses.

However, because Remote Deposit Capture can be operated from any location in the world where there is Internet access, the risk of misuse by terrorists, drug dealers, and unauthorized persons is significant.

As such, the federal agency, Federal Financial Institutions Examination Council (FFIEC)⁴⁸, has published risk management and operating guidelines that all financial institutions and their Customers must follow to keep the U.S. banking system as safe as possible and prevent financial support for unintended individuals and groups.

A new restriction of RDC is a new rule called "Exposure Limit." Financial institutions handle billions of checks each year and inspection of each check image is not humanly possible. Therefore, software systems are used to electronically monitor and control the checks as they are presented for deposit at **YOUR FINANCIAL INSTITUTION**. Each Customer of **YOUR FINANCIAL INSTITUTION** is assigned a deposit limit, which is monitored by **YOUR FINANCIAL INSTITUTION'S** system. The limit is higher than the amount normally deposited and Company will be contacted if an exception occurs.

Checks drawn on **YOUR FINANCIAL INSTITUTION** will be posted nightly to the designated account, and transit items (checks drawn on other financial institutions) will be electronically forwarded for collection via the Image Exchange Network. The Network is comprised of a group of independently operated networks, called Clearing Agents and the Federal Reserve Bank (FRB).

Remote Deposit Capture represents a key component of electronic banking. Until now, most financial institutions were chosen because of their proximity to the business. However, now any qualified business can make deposits as easily as ordering supplies over the Internet, and they are just as safe.

The benefits to Company:

- Lower cost for making deposits
- Improve availability of funds
- Improve check research with an advanced search capability
- Eliminate the liability and inconvenience of having an employee drive to make the deposit
- Avoid interrupting employees to make deposits
- Eliminate next-day deposits
- Avoid Deposit Correction fee for addition errors

Risk Management Components

In accordance with federal guidelines, "Risk Management of Remote Deposit Capture," Company is adopting the required policy and procedures to ensure the safe and legal operation of the Remote Deposit Capture System. This Policy provides guidelines to address the following

⁴⁸ "Risk Management of Remote Deposit Capture," FFIEC, January 14, 2009

requirements:

- Privacy of Information
- Document and Resource Management
- Human Resources Management
- Levels of Access Restrictions
- Information Technology Security Safeguards
- Unauthorized Access to Information (Breach) Procedures
- Vendor Oversight Management
- Business Continuity Planning

Privacy of Information

Company recognizes that protecting the privacy of our Customer's information is a foundation tenet and we take this responsibility very seriously. Each day we strive to earn and maintain that trust and confidence.

As a professional business, we require our management and staff to maintain a culture of high ethics and professionalism that our Customers expect and demand. Additionally, all of their information will be handled in a secure and confidential manner.

Title V of the Gramm-Leach-Bliley Act (GLBA) of 1999 is the legal foundation for information security for all financial institutions. This law extends to Company by Agreement with **YOUR FINANCIAL INSTITUTION** as it relates to Remote Deposit Capture. Accordingly, we will treat all non-public Customer information in compliance with all published laws and regulations.

Company will continue to protect and/or dispose of all Customer information upon the termination of the Remote Deposit Capture Agreement in accordance with this Policy.

Document and Resource Management

Company understands the risk involved in accepting and storing checks and reports related to Remote Deposit Capture and will manage all confidential documents and information accordingly.

Check Storage

At the end of each business day, the employee responsible for capturing checks using Remote Deposit Capture will ensure that checks are stored in a locked and secure filing cabinet. The checks will be placed in an envelope, or suitable storage container, with an adding machine tape or control document that lists each check captured that business day and the total amount of the deposit(s) transmitted to **YOUR FINANCIAL INSTITUTION**.

Verify Deposit Using Online System

To ensure that the correct file was updated by **YOUR FINANCIAL INSTITUTION**, a designated employee will logon to Online Banking, or system that provides appropriate information, and verify the previous day's deposit.

Check Retention and Destruction

Company will retain processed checks for _____ days as directed by management. The company will promptly provide any retained check (or, if the check is no longer in existence, a sufficient copy of the front and back of the check) to **YOUR FINANCIAL INSTITUTION** as requested to aid in the clearing and collection process or to resolve claims by third-parties with respect to any check.

Checks will be destroyed using a crisscross shredder at the expiration of their retention schedule. Company will suspend records destruction if warranted by litigation, at the request of **YOUR**

FINANCIAL INSTITUTION or regulatory requests.

All obsolete workstations or media used in the Remote Deposit Capture System will be destroyed or erased so that information cannot be read or reconstructed.

Human Resource Management

This policy section includes, by reference, Company's Human Resource Policy and extends those requirements to personnel with access to Remote Deposit Capture:

- Personnel will receive adequate training, as determined by the Human Resource Manager
- Background checks to ensure job applicants do not have criminal records
- Immediate termination of access for any employee suspected of identity theft or similar misconduct, and immediate notification to **YOUR FINANCIAL INSTITUTION**

The objectives of Company are to actively recruit, hire, and promote individuals qualified and/or trainable for positions by virtue of job-related standards of education, training, experience, and personal qualifications. However, the confidential nature of information printed on checks and related reports require the same standard of security as those that protect Company's trade secrets.

Company will conduct pre-employment background checks in an effort to hire quality employees, provide a safe environment for our customers and staff, protect the business from risk, and comply with state and federal regulations. Information collected and assessed will include verification of previous employment, criminal background, credit, and reference checks. All offers of employment are contingent upon satisfactory reports and interviews.

Employees who are terminated, or leave Company for other reasons, will be counseled that all confidential information, including trade secrets, information shown on checks or related reports may not be sold, shared, or given to any person outside Company. Violation of any unauthorized use of confidential information may result in legal actions.

Computer Software Patch Management

Company recognizes the need to establish an adequate software maintenance program. Inadequate maintenance (patching) of software exposes the company to significant risk. Software vulnerabilities may cause system unavailability, create weaknesses, or corrupt critical system components of data. Software vulnerabilities may also result in security weaknesses and can leave computer systems unprotected and open to access and criminal misuse of company information by unauthorized parties, such as computer hackers.

Authority and Responsibility

It is the responsibility of the Network Administrator to maintain current versions of software across the networks. Prior to implementing a patch, the Network Administrator will assess the impact of the application.

- The *technical evaluation* assesses whether the patch will correct a problem with the services and features of the application being used by the institution.
- The *business impact assessment* determines if applying the patch, or not applying the patch, will impact business processes and when may be an appropriate time for patch installation (i.e. immediately, after hours, over the weekend).
- The *security evaluation* determines whether there are security implications that were not identified during the technical evaluation. Even though there may be no performance benefit to applying the patch, there may be security benefits. Patches may also be identified on software that may be loaded on a system that is currently inactive.

Guidelines for Documentation

The following documentation will be maintained for the Software Patch Management Program in accordance with Company guidelines:

- Network software
- Individual software loaded on various workstations
- Versions of all software, per workstations and per network servers
- Versions of all operating systems (network and each workstation)
- Date the patch was installed
- Outstanding patches to be loaded on each specific system or workstation
- Miscellaneous information (i.e., problems encountered, reasons why the patch was not loaded (if it was not loaded), and test results if any problems arise)

Notifications of Security Patches

Several sources will be utilized in order to become aware of new patches: software vendors, network support vendors, security vendors, subscription alert services, other users, and hackers attempting to gain unauthorized access to a system.

Weekly, the network administrator will go to Microsoft.com to check for additional patches that have been released.

Procedures for Testing and Installing Patches

Each patch should be tested prior to installation to ensure that it will function as expected and be compatible with other systems.

Levels of Access Restrictions

Access to information will be restricted to information necessary for an employee to perform their duties. The Manager of Technology will review the business reasons for employees' access annually and adjust the parameters accordingly.

This policy applies to all employees and any increase of access to information requires a supervisor or manager's approval.

Information Technology Security Safeguards

IT Acceptable Use Requirements

Company is committed to protecting its employees, customers, and business partners from illegal or damaging actions. Company's systems are to be used for business purposes only in the course of normal business. Effective security is a team effort involving the participation and support of every employee who deals with information and/or information systems. It is the responsibility of every employee to adhere to the spirit of information security and to conduct their business activities accordingly.

Scope of Information Security

Information security applies to employees, contractors, consultants, temporaries, and other workers at Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company.

General Use and Ownership

- Company's management intends to provide a reasonable level of privacy, but users should be aware that the data they access from the Company's systems is the property of Company, including E-Mail.

- Any information that users consider sensitive or confidential should be encrypted when stored and not being used. Information that contains customer name, account number, financial, or tax information should be encrypted before being transmitted over the Internet.
- Employees will not install or download programs on the network or the workstation used for Remote Deposit Capture without prior approval from management. These downloads or programs specifically prohibit music, pictures, videos, or applications (software) that are illegal or not licensed Company's network or computers.
- For security and network maintenance purposes, authorized individuals within Company may monitor and audit any Company computer resource at any time.

Security/Proprietary Information

- All workstations and laptops should auto-logoff after being idle for _____ minutes
- Postings by employees using a Company E-Mail address to newsgroups or social sites are prohibited, unless posting is in the course of normal business duties.
- All computers used by the employee that are connected to the Company IT network, whether owned by the employee or the Company, shall be continually executing approved virus-scanning software with a current virus database.
- Employees are prohibited from opening E-Mail attachments, unless attachments are used in the course of normal business duties.

Unacceptable Use

Under no circumstances is an employee of Company authorized to engage in any activity that is illegal under local, state, federal, or international law while using Company-owned resources.

Prohibited Use

- Transmitting confidential information to an unauthorized person.
- Executing any form of network monitoring which will intercept data not intended for authorized use by the employee.
- Circumventing user authentication or security of any workstation, network, or account.
- Providing information about, or lists of, Company's employees or customers to an unauthorized person.

Password Requirements

- Passwords MUST be at least 8 characters in length, alphanumeric, and contain at least one special character (punctuation mark, %, \$, etc.).
- All passwords must be changed every 60 days.
- User accounts which have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into E-Mail messages, written down, or exposed in other forms of electronic communication.

Unauthorized Access of Information (Breach)

Company understands the critical roles of risk management and information security procedures to prevent identity theft and other types of illegal electronic activities. Equally important are the procedures taken if the Company experiences a breach or theft of confidential information.

Sensitive customer information means a customer's name, address, telephone number, social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password, which would permit unauthorized access to information.

As a directive of this Policy, if management has a suspicion, or becomes aware of an actual incident, an aggressive investigation will commence immediately in accordance with published federal and state guidelines. The conclusion of the investigation will result in appropriate actions:

- No actual breach—notification to management of the findings of the investigation and possible future actions
- Breach in progress—collection of forensic data for law enforcement agencies, shut down Internet access and internal network, internal audit of systems, determination of extent of breach, and notification to **YOUR FINANCIAL INSTITUTION** of breach.
- Evidence that Breach Occurred—collection of forensic data for law enforcement agencies, shut down Internet access and internal network, internal audit of systems, determination of extent of breach, consultation of management and corporate attorney, notification to **YOUR FINANCIAL INSTITUTION** of breach, and possible notification to affected customers.

The method of communications to customers, when warranted, will be the sole responsibility of Company management. Retention of investigation data will be seven (7) years.

To comply with Company's guidelines for managing an effective Risk Management Program, the Company will require its "mission critical" vendors to notify Company if it experiences a security breach and take appropriate actions to address an incident of unauthorized access to confidential information relating to Company.

Vendor Oversight

Oversight is a critical step in managing Company's risk management program, which includes the process of identifying, measuring, monitoring, and controlling the risks associated with outsourcing technology services. Since Oversight covers a broad range of issues that should be addressed, the Company has defined the appropriate elements based on the scope and importance of the outsourced services as well as the associated risk to the company.

Vendor selection during technology acquisitions will include careful screening of proposing vendors to ensure that the company selected has strong management, a corporate culture of high ethics, as well as quality products and services.

The following information will be required or compiled for analysis of "mission critical" vendors:

- Financial statements
- Copies of any security related audits
- Verifiable references (to establish the reputation of the vendor)

Rankings of vendors will be based on the access they have to confidential information:

- Mission critical and significant access to confidential information

Vendors in this category will be reviewed annually for creditworthiness and compliance with our policy regarding vendor access to non-public information. Vendors must also have a policy and include in their agreement with Company that they will not sell, share, or disclose any non-public information they are provided, obtain, or discover during assignments or while providing products or services to Company.

- Important vendors with minimal access to confidential information

Vendors in this category will be reviewed annually regarding vendor access to non-public information. Vendors must also have a policy and include in their agreement with Company that they will not sell, share, or disclose any non-public information they are provided, obtain, or discover during assignments or while providing products or services to Company.

- Important vendors that do not have access to confidential information

Vendors in this category will be listed on Company's vendor analysis tracking report, but are not

required to provide information about their company or individuals.

Annual Report of Findings

The findings of all reviews will determine any action that is necessary and will be presented in a summary report to the Board (**Senior Management**).

Alternate Deposit Plan

Company management understands that implementing Remote Deposit Capture has changed the processes previously used to make deposits at **YOUR FINANCIAL INSTITUTION** and plans to use the following alternative in the event of an outage that prevents normal operation of RDC:

- Office of **YOUR FINANCIAL INSTITUTION** is within driving distance and an employee will make the deposit by driving to the nearest branch.
- **OPTIONAL**—Office of **YOUR FINANCIAL INSTITUTION** is not within driving distance and an overnight delivery service will be used to make a “mail deposit.”

Company and financial institution will mutually agree upon the reason for the outage and the party responsible will pay for the cost of the overnight delivery service.

Employee Training

At the initial installation of the RDC System, Company will receive sufficient training to properly operate the RDC system and understand the related Rules and Regulations. Annually, thereafter, Company will receive an update to the Training Program, in the form selected by the **YOUR FINANCIAL INSTITUTION**, that explains all of the changes that have occurred in the system, procedures, law, or regulation that pertain to RDC.

Authority and Review

Changes to this Policy require approval by the Board of Directors (**Senior Management**) of Company. Changes in operating procedures, standards, guidelines, and technology, provided they are consistent with this policy, may be authorized by Company's Operations Manager.

While there are inherent risks with any type of business system, RDC offers Company considerable flexibility in making deposits, controlling costs, and managing cash flow. For strategic and operating reasons defined in this document, the Board of Directors (**Senior Management**) approved this policy and related procedures.

Approved by: _____

Title: _____

REMOTE DEPOSIT CAPTURE PROCEDURES

An overview

The FFIEC published the “Risk Assessment for Remote Deposit Capture,” which defines how certain businesses and consumers must develop, implement, and administer their Risk Management program.

Your program must include reasonable policies and procedures to ensure that customer check information is kept secured until it is destroyed. For example, in the day-to-day operation of the Remote Deposit Capture system there will be times when an employee must leave his or her work area, such as breaks, lunch, or running business errands. When these situations occur, it is imperative that the Remote Deposit Capture workstation is logged off and only an employee with authorized credentials can restart the workstation.

Preventing Identity Theft

The checks you capture today using Remote Deposit Capture can provide most of the information needed to create a fraudulent identity. Because of the sensitivity of customer information, each employee handling the checks must be trained to protect confidential information.

Skilled identity thieves⁴⁹ use a variety of ways to gain access to personal information. For example, they may get information from businesses or financial institutions by stealing it while they’re on the job, bribing an employee who has access to these records, hacking these records, and conning information out of employees. Or:

- They may steal your wallet or purse
- They may steal your personal information through email or the phone by saying they’re from a legitimate company and claiming that you have a problem with your account. This practice is known as “phishing” online, or “pretexting” by phone.
- They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as “skimming.” They may swipe your card for an actual purchase, or attach a device to an ATM machine where they may enter or swipe your card.
- They may get your credit reports by abusing the authorized access that was granted to their employer, or by posing as a landlord, employer, or someone else who may have a legal right to your report.
- They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as “dumpster diving.”

The following procedures are intended to assist you in establishing and maintaining your RDC process. As you study the procedures, change them to best fit your company or situation.

⁴⁹ Source: Federal Trade Commission, “*Fighting Fraud with the Red Flag Rule*”

Daily Procedures

Activity	Department	
Planning the day's activities		
Verify previous day's deposit to online banking		
Verify Deposit Acknowledgement was completed from the previous day and entered into the Daily Processing Log		
Review system and security reports		
Prepare checks for processing		
Use endorsement stamp		
Create a control document		
Clean scanner		
Jog checks ⁵⁰		
Capture Checks		
Verify image quality		
Update Daily Processing Log		
Store checks in locked file cabinet		
Destroy checks in accordance with Check Retention Policy		
Ensure backups are competed and rotated		

⁵⁰ Depending on your volume and scanner

Planning the Day's Activities



Each day, the operator and Remote Deposit Capture manager should review the following:

- Daily processing
- Changes in processing
- Procedural changes
- Training for security

It is also a great time to discuss issues that may be of concern to the operator or financial institution, such as balancing problems or image quality. Recording any issue on an “Operator’s Log” is the best way to track problems over time. If it is not written down immediately after it happens, the operator may forget it. The Operator’s Log can be part of the agenda for vendor and staff meetings.

Notes:

Verify Previous Day's Deposit



Each day, the Accounting Manager, or designee, should verify that the previous day's checks were electronically deposited correctly at the financial institution.

Logon to Online Banking and verify the check capture deposit(s) from the previous day equals the total from the adding machine tape (Control Document) created during the previous day's check preparation step. If for any reason the totals do not match, contact Customer Service at the number provided by your financial institution.

Identifying and resolving issues with the latest deposit is usually fast and simple instead of having to research items that may have been destroyed once the retention period has expired.

By taking a few minutes each day to verify the total of the last RDC deposit with online banking, you may detect a problem and avoid significant research time later. This is the final step from the previous day's processing, and there are other balance points described in this document to help you detect any problem that may keep your deposit from reaching the financial institution successfully.

There are also other reasons that deposits are not transmitted: distractions caused by workplace interruptions, employee illness, or the operator simply forgetting to transmit the deposit. RDC systems are designed to detect duplicate items, but not transmissions that were not made.

Notes:

Verify Previous Day's Deposit Acknowledgement was Filed



The Deposit Acknowledgement is a legal term that is incorporated in the language of your Deposit Account Agreement. It is the switch that turns over the responsibility for properly handling the checks in the RDC transmission from the customer to the financial institution. When the acknowledgement occurs, a communication of receipt is provided to the customer. The communication may be in the form of an E-mail, transmission, display, or contained in a report that should be printed.

Prior to the financial institution signaling that they have received and accept the checks, the customer is still responsible for anything that happens before receiving the acknowledgement.

For example, if the customer's Internet Service Provider (ISP) experiences an outage, the transmission may not occur and the financial institution will not receive the transmission. Therefore, the financial institution cannot be held liable for not transferring the deposit and checks to the proper accounts or to other financial institutions where items may be drawn.

This electronic procedure replaces the teller giving a customer a receipt when they make an over-the-counter paper-check deposit.

Notes:

Review System and Security Reports



Computers are used for everything from selling products and services, ordering supplies, sending E-mail, online banking, and RDC. In the hectic pace in most companies, important signals that someone is trying to access information that your company may deem confidential, including trade secrets, may be overlooked unless there is an established procedure for reviewing available security reports that monitor such activities.

Reviewing the usage and security reports generated or available from the RDC system, workstation, or network is one of the best “early detection” procedures available to RDC customers. The goal of the daily review is to detect any anomalies that may be the result of an unauthorized access attempt, such as a hacker. Best practices for security would include the daily review of available reports:

- Network security and attempts to breach the firewall
- Unauthorized login attempts on the network (internal fraud attempt)
- Numerous login attempts on the RDC system by an unauthorized employee
- Attempts by an employee to access restricted information
- Virus and malware detection
- RDC security reports

Effective security is not the result of one system or procedure, but the use of all available reports and systems and daily review of their findings for detecting unauthorized attempts to access your systems.

Notes:

Preparing Checks for Processing



Preparing checks for processing is an important step for RDC. Customers are prone to stapling or using gem clips to attach a bill to the check. The concern may be that the bill and check can be separated and they may not receive proper credit. However, staples and gem clips can wreak havoc on the small digital camera inside the scanner.

When preparing the checks for scanning:

- Inspect and remove gem clips, staples, and rubber bands
- Make sure there is no adhesive material on the front or back of any check
- Turn each check right-side up

Damaged or Unsigned Checks

Sometimes you will receive checks that have been torn or crumpled to the point of being unusable. Try to smooth out the checks before scanning them. In some cases, you may have to use Scotch Clear Tape to repair the checks before scanning them. If a check has significant quality issues or is not signed, you should contact the checkwriter for a replacement.

Notes:

Use Endorsement Printer

One of the best fraud detection techniques is usually built into the scanner, printing the endorsement on the back of the check during capture.

As the check passes through the scanner, the inkjet printer, which is located inside the scanner and will print endorsement information⁵¹ that identifies the check as having been electronically captured and processed by your financial institution.

Example: *This Check Has Been Electronically Captured by First National Bank of Anytown, Texas*

The endorsement printing by the scanner may alert a teller that this check has been previously deposited electronically and possibly prevent a check stolen from your company to be fraudulently deposited again.

Notes:

⁵¹ Endorsement printing is vendor dependent. Contact your RDC vendor for additional information.

Create a Control Document



Something as simple as an adding machine tape can become one of the most important controls in RDC. By using the adding machine tape as a “control document,” you can ensure that the integrity of the checks in the deposit is maintained as they move through the process.

The tape is first used to provide a list of checks and a balancing total for comparing the checks read by the scanner. Sometimes, the scanner may misread a check amount, skip a check, or encounter a piggyback (overlapping checks). These types of problems are detected during the balancing step when the operator compares the captured checks report to the adding machine tape.

Use a control document at the following steps:

- When a batch/run is initiated the system will ask for a deposit total
- When the captured checks/deposit are transmitted to the financial institution and you are provided with an deposit acknowledgement (receipt)
- The next day when the deposit is verified using online banking

Notes:

Equipment Maintenance

1-Open Case



2



3



4-Use Air to Remove Dust



Although there are numerous scanner vendors and models, most maintenance⁵² is similar. Because the scanners were designed to be maintained by customers, opening the cases and cleaning them is fast and simple.

It is important to clean your scanner each day. As you scan checks, small particles of paper separate from the checks and can settle on the camera lens and impair the quality of the images. In addition, you should wipe the outside case with a lint-free cloth to remove any dust or particles that may find their way into the scanner.

⁵² Refer to the vendor's maintenance guide provided for your brand and model

5–Use Alcohol to Clean Dirty Mirrors



6–Finished and Ready to Test



For scanners with extended mirror cases, you may need to wipe the mirrors with a lint-free cloth and alcohol or run a scanner-cleaning card through the machine. Although alcohol may be used for mirrors—it has a tendency to dry out rubber-based parts, such as belts and rollers (Consult your cleaning Guide for instructions).

With the exception of the Cleaning Card,⁵³ cleaning supplies can normally be purchased from office supply stores.

Typical Supply List:

1. Inkjet Cartridge
2. Replacement Rollers
3. Q-Tips
4. Alcohol
5. Lint-free cleaning cloths
6. Soft brush
7. Can compressed air-spray
8. Cleaning Card

All of the scanners sold today have a long life expectancy. It usually the belt and rollers that dry out before they wear out⁵⁴ and should be inspected and replaced as needed.

Notes:

⁵³ Cleaning Cards should be purchased from the manufacturer of the scanner

⁵⁴ Determined by the daily number of checks captured

Jog Checks



Joggers are machines that vibrate intensely and separate checks that may stick together due to static electricity or an adhesive on the front or back of a check. They are not necessary for hand-fed scanners or low check volumes. Some scanner manufacturers have built-in joggers that are used immediately before actually capturing the checks.

For high volume businesses, joggers are invaluable for preventing piggyback checks that may create additional research.

Notes:

Capture Checks



This is the heart of Remote Deposit Capture, scanning and capturing checks using a small desktop scanner and transmitting the high resolution images to a financial institution. Image technology is not new, but the combination of advanced technology, advanced system software, and a check law to “foster innovation”⁵⁵ has created an epoch in item processing. Although RDC does not reduce the number of checks processed, it streamlines the requirement for making a deposit and lowers the item processing cost.

Fraud is Reduced with Remote Deposit Capture

The concern of federal and state regulators is RDC may be used for fraudulent purposes. However, according to the FDIC, “To date, the federal financial institution regulatory agencies have not observed increased fraud rates related to RDC services. In fact, the RDC fraud rate is lower than the average for general item processing.”⁵⁶

Notes:

⁵⁵ Check 21 Act, page 1, paragraph 1

⁵⁶ FDIC Supervisory Insights Summer 2009, page 21

Verify Image Quality

#1 – Good Image



#2 – Poor Image

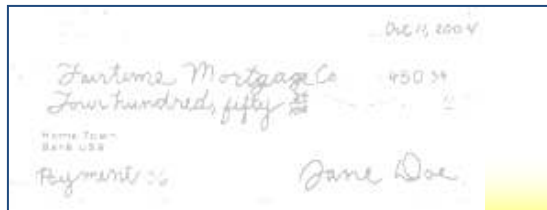


Image quality may be the most important component of check scanning and each day you should test the quality to ensure that the system and scanner are working properly.

After you clean the scanner, look at the quality of a captured check. If it looks great, it is time to go to work. If the image is not acceptable, clean the machine again and retest. Daily scanning should not begin until the image quality is excellent.

When you have cleaned the scanner a second time and the quality does not improve, call Customer Support at the number provided by your financial institution for the next level of diagnosis.

Notes:

Daily Processing Log



Daily Processing Log

Date	Employee	Check/ Run #	Batch #	Trans. Count	Deposit Amount	Confirm Number	Comments

It is important to document the pertinent information about the checks and deposits each time they are handled. In the event of an error, having the information from the Daily Processing Log could reduce the research time required to resolve all types of problems: missing deposit, deposit correction error, or having to resubmit a file due to an error with the Internet Service Provider (ISP).

Notes:

Store Checks in Safe Place

1. Place captured checks in an envelope or box labeled with the capture date and destroy date.



2. Place the envelope or box in a filing cabinet or safe container that is not generally available to the public.



3. Lock the file cabinet or container.



Every step must be taken to ensure that checks and the information they represent are kept safe and one of the most effective tools is a checklist. Checklists are used in thousands of companies and industries because they work and prevent employees from forgetting to complete an important task.

No pilot would consider flying a plane without first using a checklist to ensure that each component is working properly. The same is true with RDC and its checklist. With a checklist, like the one above, you can review each step and ensure that the important steps are completed.

Take the time to make sure you inspect your system and security controls to keep hackers and fraudsters on the outside of your company.

Notes:

Shredding Checks



Your retention guideline should define how long you keep the original checks before destroying them.

As discussed at the beginning of this chapter, identity thieves are on a constant search for confidential information. They know all the places that people dispose of documents, including checks. In fact, many people do not use their checking statements and simply toss them into the trash. Stealing a statement provides a thief with a person's name, address, account number, and financial institution. The only piece of information missing is the social security number for a fraudster to begin opening accounts in the victim's name.

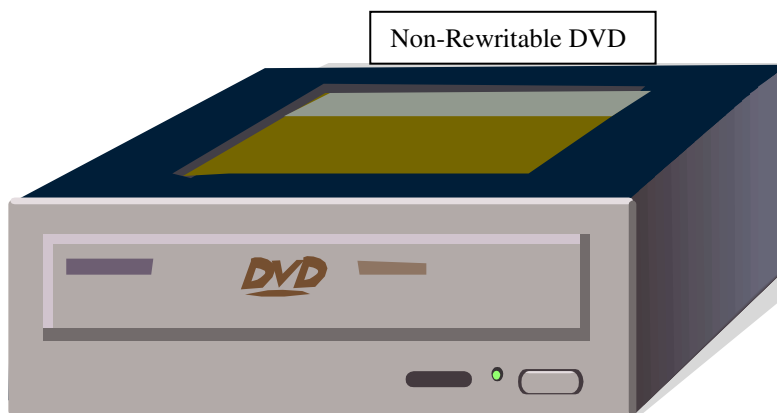
When shredding checks, it is best to use a crisscross shredder to prevent checks from being reconstructed. Once shredded, they can be disposed of in any process that allows paper chads (very small pieces of paper).

Because of the prevalence and seriousness of identity theft, the FFIEC requires every financial institution to include language in the RDC Agreement that requires each customer to have a security procedure that keeps information safe: "Handling and record retention procedures for the information in RDC, including physical and logical security expectations for access, transmission, storage, and disposal of deposit items containing nonpublic personal information."⁵⁷

Notes:

⁵⁷ FFIEC Risk Assessment for Remote Deposit Capture, January 14, 2009, page 7

Daily Backup and Archive



Like other features and functions in RDC, the technique for storing images is vendor dependent.⁵⁸ Some vendors store 30-days of images on the RDC workstation and some do not store any. You need to understand how your system works and perform daily backup accordingly.

If you store and use the check images from your RDC workstation, a backup copy of the images should be created daily and stored off-site in the event of an emergency, such as a fire or tornado. The backup can be included in the normal network backup if the RDC workstation is part of that domain.

The backup media, like your network backup, should be protected during creation, transport, and storage and you should test it annually to ensure the copy procedure is operating properly.

It is important to note that your financial institution also maintains an archive copy of all of your deposits and check images. Additionally, they are required by federal and state regulators to annually test their backups to ensure the integrity of the backup files.

If needed, your financial institution can convert an image into a substitute check, which has the same legal standing as the original check, regardless of when it was created.

Notes:

⁵⁸ Discuss data image backup and archive requirements with your RDC vendor or financial institution

TRAINING QUESTIONS AND ANSWERS

Frequently Asked Questions about Check 21 Act (FAQs)

Source: Federal Reserve Bank: <http://www.federalreserve.gov/paymentsystems/truncation/faqs2.htm#ques1>

1. What is Check 21 Act and what is its basic purpose?

Check 21 Act is a federal law that is designed to enable banks to handle more checks electronically, which should make check processing faster and more efficient. Today, banks often must physically move original paper checks from the bank where the checks are deposited to the bank that pays them. This transportation can be inefficient and costly. Check 21 Act became effective on October 28, 2004.

2. How will Check 21 Act make check processing more efficient?

Instead of physically moving paper checks from one bank to another, Check 21 Act will allow banks to process more checks electronically. Banks can capture a picture of the front and back of the check along with the associated payment information and transmit this information electronically. If a receiving bank or its customer requires a paper check, the bank can use the electronic picture and payment information to create a paper "substitute check." This process enables banks to reduce the cost of physically handling and transporting original paper checks, which can be very expensive.

3. Is electronic check processing secure?

Electronic check processing is not new to the financial industry and is a safe and reliable way of processing payments. It uses technology that has been developed and tested to process your check information securely.

4. Does Check 21 Act mean that customers can't get their checks back in their account statements?

No. Check 21 Act does not require customers to stop receiving checks back in their account statements. The contents of an account statement will continue to be governed by the account agreement between the bank and its customer. Rather, when banks have agreed to provide paid checks in statements, Check 21 Act permits the bank to provide either the original check or a substitute check.

5. What changes can I expect when Check 21 Act goes into effect?

If you are among the many customers of banks that do not receive your canceled checks with your account statement, you likely will not notice any change when Check 21 Act goes into effect on October 28, 2004. You will notice a change only if you receive a substitute check when you were expecting an original check. For example, if you receive canceled checks with your account statement, you might begin to receive a mixture of canceled original and substitute checks. If you receive image statements (pictures of several checks on a single page), you also may notice that some of the pictures are of substitute checks.

6. Will Check 21 Act increase the speed with which checks are cleared between banks?

The speed of check processing already has increased in response to check system improvements other than Check 21 Act. Thus, even now, once a check is deposited with a bank, it is almost always delivered overnight to the paying bank and debited from the checkwriter's account the next business day. Check-processing speeds should continue to increase, over time, as banks make further operational changes in response to Check 21 Act. That means money may be deducted from your checking account faster.

Before you write a check, it's always best to make sure your checking account has enough money in it to cover the check.

7. Will Check 21 Act change how fast my bank must make my check deposits available for withdrawal?

Another federal check law (the Expedited Funds Availability Act) specifies the maximum times by which your bank must make funds available to you, though most banks make funds available faster than required. Check 21 Act did not change these maximum hold times. However, the Expedited Funds Availability Act requires the Federal Reserve Board to reduce maximum hold times in step with reductions in actual check-processing times. Thus, over the longer term, if Check 21 Act sufficiently increases the speed of check processing, the Board will reduce maximum hold times.

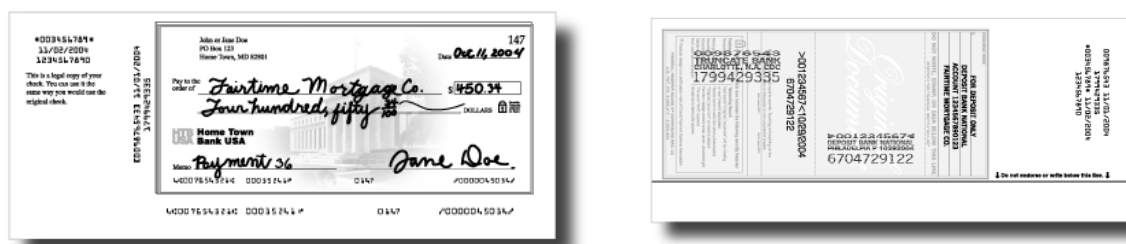
A bank's decision to place a hold on funds you deposit by check does not affect the interest that you receive on the deposited funds. Specifically, if you deposit a check into an interest bearing checking account, your bank is generally required to begin to credit interest to your account no later than the business day on which the bank receives credit for the funds.

8. What is the difference between Check 21 Act and programs that convert checks to electronic payments?

A check you write may be processed as a check. In that case, your rights are governed by check laws and regulations. Some merchants, however, may use your check as a source of information to create an electronic fund transfer. You must receive notice that your check may be processed this way. Electronic fund transfers are governed by different laws and have different consumer rights than check payments. For more information, see the brochure "[When Is Your Check Not a Check: Electronic Check Conversion](#)" published by the Federal Reserve Board.

9. What is a substitute check?

A substitute check is a paper copy of the front and back of the original check. A substitute check is slightly larger than a standard personal check so that it can contain a picture of your original check. A substitute check must be printed in accordance with very specific standards so that the substitute check can be used in the same way as the original check. If you receive a substitute check that appears to have a problem, such as it contains a bad picture of your original check, contact your bank.



10. When is a substitute check legally the same as the original check?

A substitute check is legally the same as the original check if it accurately represents the information on the original check and includes the following statement: "This is a legal copy of your check. You can use

it the same way you would use the original check.” The substitute check must also have been handled by a bank.

If you receive a substitute check that is not legally the same as the original check and you suffer a loss related to the substitute check, Check 21 Act provides you with a special procedure that you can use to get your money back.

11. Can I use a substitute check as proof of payment?

Yes. You can use a substitute check as proof of payment because it is legally the same as the original check. For instance, the IRS will accept your substitute check as proof of payment. If you do not have a substitute check but have a copy of an original check or a copy of a substitute check, you usually can use these documents as proof of payment.

12. How are image statements different from substitute checks?

Instead of providing canceled checks, some banks provide customers with image statements that show multiple pictures of canceled checks per page. The pictures on the image statement could represent an original check or a substitute check. Whether the consumer receives an original check, a substitute check, an image statement, or a line item on his or her account statement, check law protects consumers against erroneous and unauthorized check payments. In addition, Check 21 Act provides a special refund procedure (called “expedited recredit”), if you receive a substitute check.

13. Can I demand a substitute check from my bank instead of a copy?

Your bank may provide you with a substitute check, but it is not required by law to do so. If your bank does not provide you with a substitute check, you usually can use a copy of an original check or a copy of a substitute check as your proof of payment.

14. What should I do if something is wrong with the substitute check that I receive?

A substitute check must show the front and back of the original check and be printed in accordance with very specific standards. If you receive a substitute check that appears to have a problem, such as it contains a bad picture of your original check, contact your bank.

15. Is my bank required to tell me about substitute checks?

Under Check 21 Act, banks are required to provide a disclosure to their consumer customers who receive canceled checks with their monthly statements. The disclosure describes substitute checks and consumer rights regarding substitute checks. Banks must provide this disclosure to existing customers not later than the first statement mailing after Check 21 Act becomes effective on October 28, 2004. After October 28, 2004, banks must provide this disclosure to new customers at the time the customer relationship is established. If you receive canceled checks with your account statement but did not receive the required disclosure within the timeframes described above, please request one from your bank.

Banks must also provide this disclosure when a consumer requests an original check or copy of a check and receives a substitute check. In addition, the bank must provide this disclosure if a check the consumer has deposited is returned unpaid to the consumer in the form of a substitute check.

16. Can I still get my canceled checks back?

If you get your canceled checks back with your account statements today, you will continue to receive canceled checks unless your bank notifies you otherwise. The only difference will be that some of the canceled checks that you receive may be substitute checks. You can use a substitute check the same way you would use an original check, such as for recordkeeping and proof-of-payment purposes.

17. Can I get my original check if I need it?

Banks are not required currently to keep your original check for any specific length of time, and Check 21 Act does not add any new retention requirements. In many cases, the original check may be destroyed. If you request your original check from your bank, your bank may provide you with the original check, a substitute check, or a copy of the check.

18. Can I prevent others from using my original check to create a substitute check?

No. Generally, any check can be used to create a substitute check, except a foreign check. Banks and their customers must accept a substitute check as if it were the original check because the substitute check is legally the same as the original check.

19. What if I receive a substitute check representing a fraudulent original check?

Check law provides protections against fraudulent checks so that generally you are not responsible if you notify the bank in a timely fashion. This is the case whether you receive an original check, a substitute check, an image statement, or a line item on your account statement. If you receive a substitute check of a fraudulent original check, you may have additional rights under Check 21 Act. Contact your bank for more information.

20. Do I need to use magnetic ink or toner when printing checks?

To process checks, banks' automated check sorting equipment relies on numeric information that appears at the bottom of checks and is printed in magnetic ink. This information is known as the check's magnetic ink character recognition line, or MICR line, and contains information such as the routing number of the bank on which the check is drawn, the account number on which the check is drawn, and the check serial number. Generally applicable industry standards for original checks long have required the MICR line to be printed in magnetic ink; the need for magnetic ink on original checks is not the result of the Check 21 Act. Only the MICR line of a check must be printed in magnetic ink. The rest of the information on the check, such as the date, the payee name, and the amount, can be printed in regular, non-magnetic ink.

If you make payments by printing checks at home and the checks you use have pre-printed MICR lines, then the rest of the information that you print on the checks need not be in magnetic ink. By contrast, if you must print a check's MICR line because it is not preprinted on the check, you should print the MICR line in magnetic ink.

21. How am I protected under Check 21 Act?

Check law protects you against erroneous and unauthorized check payments. In addition, Check 21 Act contains a number of new protections for consumers. For example, Check 21 Act contains a special refund procedure (called "expedited recredit") for a consumer who suffers a loss related to a substitute check he or she received.

22. What protections do I have if I receive image statements, access pictures of my checks online, or receive an account statement with descriptive information about my canceled checks?

Years ago, many banks stopped providing customers with canceled checks and, as an alternative, began providing customers with documentation showing which checks were paid. Regardless of the form of documentation you receive, check law protects you against erroneous and unauthorized check payments.

23. If I suffer a loss related to a substitute check I received, can I file a claim with my bank?

Yes. If you have received a substitute check, you can file a special claim with your bank for a refund (called an “expedited recredit”) if you believe that:

- The substitute check was incorrectly charged to your account,
- You lost money as a result of the substitute check being charged to your account, and
- You need the original check or a copy sufficient to show that the substitute check was incorrectly charged to your account.

24. Does the special refund procedure apply if I receive an image statement with a picture of a substitute check but do not receive the actual substitute check?

No. The special refund procedure applies only if you actually received a substitute check. However, check law protects you from improper check charges regardless of whether you receive an original check, substitute check, image statement, or a line item on your account statement. If you feel an error was made to your account, contact your bank immediately.

25. How do I make a claim under the Check 21 Act refund procedure?

If you believe that you have suffered a loss relating to a substitute check that you received, you should contact your bank as soon as possible but no later than 40 days from when your bank mailed or delivered your account statement. Your bank will ask you to provide information it needs to investigate your claim, which could include a description of the problem, an estimate of your loss, and information about the substitute check.

26. How quickly must my bank handle my claim, and when will my account be refunded?

Your bank should investigate your claim promptly. If your bank finds that it incorrectly charged your account, the bank must refund the amount of your claim (up to the amount of the substitute check, plus interest if your account earns interest) within one business day of making that decision.

If your bank is unable to determine the validity of your claim within 10 business days after receiving it, your bank on that day must refund the amount of your loss up to the lesser of amount of the substitute check or \$2,500, plus interest (if your account earns interest). Unless your bank determines that your claim is not valid, it must refund to your account any remaining amount of your loss, up to the amount of the substitute check, plus interest, no later than the 45th calendar day after the bank received your claim.

If your bank later determines that your claim was not valid, it may reverse the refund and interest it has paid to you.

27. How will I know if my bank has refunded my account?

If your bank refunds your account, it will send you a notice by the next business day that tells you the amount of your refund and the date on which you may withdraw those funds. Normally, you may withdraw your refund on the business day after your bank refunds your account.

28. Can my bank delay my ability to withdraw the amount that it refunds?

If your bank is still investigating your claim, it may delay your ability to withdraw up to the first \$2,500 of the refund if (1) you are a new accountholder, (2) your account is repeatedly overdrawn, or (3) the bank has reason to believe the claim is fraudulent. In these cases, your bank must allow you to withdraw the funds after determining that your claim is valid or on the 45th calendar day after the day that you submitted your claim, whichever occurs first.

29. What happens if my bank says it charged my account correctly?

If your bank determines that it correctly charged your account, it will send you a notice by the next business day that explains the reason for that decision and will include either the original check or a copy of the original check that is sufficient to determine the validity of your claim. Your bank will also either include the documentation the bank used in making its determination or will explain that you can request such documentation.

PowerPoint Training Program

On the CD provided with this Binder is a Microsoft PowerPoint© ***“2009 Remote Deposit Capture Rules & Training Guide©”***. The material is published and printed in the USA and marketed worldwide. Copyright © 2009 by T. Houston Technology Group. All rights reserved. No part of this book or CD and related materials may be reproduced or transmitted in any form or by any means electronic or mechanical, including photocopying, recording, or by any informational storage or retrieval system without written permission from the publisher, except for brief quotations used in critical articles and reviews. For information contact: T. Houston Technology Group, P.O. Box 1727, Alvin, Texas 77512. Telephone (281) 756-0409 or email: thouston@thouston.com.

For additional project team copies, or corporate subscriptions, contact the above numbers, but do not make any additional copies of the book or pages.

REFERENCES OF APPLICABLE RULES AND REGULATIONS

The “Risk Management of Remote Deposit Capture” was published on January 14, 2009, by the Federal Financial Institutions Examination Council to provide the foundation on which financial institutions and their customers could develop and implement appropriate policies and procedures. The interagencies are responsible for designated financial institutions and publish their guidelines accordingly.

Federal Financial Institutions Examination Council (FFIEC)



“The Federal Financial Institutions Examination Council (FFIEC) was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) established The Appraisal Subcommittee (ASC) within the Examination Council.

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.”⁵⁹

Federal Deposit Insurance Corporation (FDIC)



“The Federal Deposit Insurance Corporation (FDIC) preserves and promotes public confidence in the U.S. financial system by insuring deposits in banks and thrift institutions for at least \$250,000; by identifying, monitoring and addressing risks to the deposit insurance funds; and by limiting the effect on the economy and the financial system when a bank or thrift institution fails.

An independent agency of the federal government, the FDIC was created in 1933 in response to the thousands of bank failures that occurred in the 1920s and early 1930s. Since the start of FDIC insurance on January 1, 1934, no depositor has lost a single cent of insured funds as a result of a failure.

The FDIC receives no Congressional appropriations—it is funded by premiums that banks and thrift institutions pay for deposit insurance coverage and from earnings on investments in U.S. Treasury securities. With an insurance fund totaling more than \$17.3 billion, the FDIC insures more than \$4 trillion of deposits in U.S. banks and thrifts—deposits in virtually every bank and thrift in the country.

Savings, checking and other deposit accounts, when combined, are generally insured to \$250,000 per depositor in each bank or thrift the FDIC insures.

⁵⁹ <http://www.ffiec.gov/about.htm> (Accessed August 20, 2009)

The standard insurance amount of \$250,000 per depositor is in effect through December 31, 2013. On January 1, 2014, the standard insurance amount will return to \$100,000 per depositor for all account categories except IRAs and other certain retirement accounts, which will remain at \$250,000 per depositor. Deposits held in different categories of ownership – such as single or joint accounts – may be separately insured. The FDIC's Electronic Deposit Insurance Estimator can help you determine if you have adequate deposit insurance for your accounts.

The FDIC insures deposits only. It does not insure securities, mutual funds or similar types of investments that banks and thrift institutions may offer. ([Insured and Uninsured Investments](#) distinguish between what is and is not protected by FDIC insurance.)

The FDIC directly examines and supervises about 5,160 banks and savings banks, more than half of the institutions in the banking system. Banks can be chartered by the states or by the federal government. Banks chartered by states also have the choice of whether to join the Federal Reserve System. The FDIC is the primary federal regulator of banks that are chartered by the states that do not join the Federal Reserve System. In addition, the FDIC is the back-up supervisor for the remaining insured banks and thrift institutions.

The FDIC is managed by a five-person [Board of Directors](#), all of whom are appointed by the President and confirmed by the Senate, with no more than three being from the same political party.”⁶⁰

Federal Reserve Bank (FED)

Congress created the Federal Reserve System in 1913 to serve as the central bank of the United States and to provide the nation with a safer, more flexible and more stable monetary and financial system. Over the



years, the Fed's role in banking and the economy has expanded, but its focus has remained the same. Today, the Fed's three functions are:

- To conduct the nation's monetary policy,
- To provide and maintain an effective and efficient payments system, and
- To supervise and regulate banking operations.

Although all three roles are important in maintaining a stable growing economy, monetary policy is the most visible to many citizens. Monetary policy is the strategic actions taken by the Federal Reserve to influence the supply of money and credit in order to foster price stability and maintain maximum sustainable economic growth. Through these actions, the Fed helps keep our national economy strong and the world economy stable.”⁶¹

National Credit Union Administration (NCUA)



“The National Credit Union Administration (NCUA) is the independent federal agency that charters and supervises federal credit unions throughout the United States and its territories.

⁶⁰ <http://www.fdic.gov/about/learn/symbol/index.html> (Accessed August 20, 2009)

⁶¹ <http://www.phil.frb.org/about-the-fed/introduction> (Accessed August 20, 2009)

NCUA administers the National Credit Union Share Insurance Fund (NCUSIF). Backed by the full faith and credit of the United States government, the NCUSIF insures the member accounts in all federal credit unions and the substantial majority of state-chartered credit unions.”⁶²

The Office of the Comptroller of the Currency (OCC)



“The Office of the Comptroller of the Currency (OCC) charters, regulates, and supervises all national banks. It also supervises the federal branches and agencies of foreign banks.

Headquartered in Washington, D.C., the OCC has four district offices plus an office in London to supervise the international activities of national banks.

The OCC was established in 1863 as a bureau of the U.S. Department of the Treasury. The OCC is headed by the [Comptroller](#) , who is appointed by the President, with the

advice and consent of the Senate, for a five-year term. The Comptroller also serves as a director of the Federal Deposit Insurance Corporation (FDIC) and a director of the Neighborhood Reinvestment Corporation.

The OCC's nationwide staff of examiners conducts on-site reviews of national banks and provides sustained supervision of bank operations. The agency issues rules, legal interpretations, and corporate decisions concerning banking, bank investments, bank community development activities, and other aspects of bank operations.

National bank examiners supervise domestic and international activities of national banks and perform corporate analyses. Examiners analyze a bank's loan and investment portfolios, funds management, capital, earnings, liquidity, sensitivity to market risk, and compliance with consumer banking laws, including the Community Reinvestment Act. They review the bank's internal controls, internal and external audit, and compliance with law. They also evaluate bank management's ability to identify and control risk.”⁶³

Office of Thrift Supervision (OTS)



“The OTS supervises a national thrift industry that is built on the bedrock of the American dream of homeownership—supplying affordable home financing for Americans from all walks of life.

The industry has a long history dating back to 1831 with the establishment of the first savings association, the Oxford Provident Building Association, which made home loans and offered savings accounts. Today, the charter is a vibrant, sophisticated model for running a retail financial services business.”⁶⁴

⁶² <http://www.ncua.gov> (Accessed August 20, 2009)

⁶³ <http://www.occ.gov/aboutocc.htm> (Accessed August 18, 2009)

⁶⁴ <http://www.ots.gov/?p=AboutOTS> (Accessed August 20, 2009)

State Departments of Banking



Each state has a Department of Banking⁶⁵ that examines each state bank in their state.

Agency Mission:

Our mission is to ensure Texas has a safe, sound and competitive financial services system.

Agency Philosophy:

- Adhere to the highest ethical and professional standards;
- Be accountable and responsible;
- Anticipate and respond to a dynamic environment;
- Identify and promote innovative practices;
- Operate efficiently;
- Communicate effectively;
- Foster teamwork;
- Promote individual excellence and career development;
- Provide a desirable work environment that values cultural and individual differences; and
- Seek input from and be responsive to the public, our supervised entities, and State leadership.

⁶⁵ Texas Department of Banking was selected as an example
<http://www.banking.state.tx.us> (Accessed August 20, 2009)

RISK MANAGEMENT OF REMOTE DEPOSIT CAPTURE

Quick Reference

SECTION	REFERENCE DOCUMENTS
Risk Management: Risk Assessment	<i>FFIEC IT Examination Handbook</i> http://www.ffiec.gov/ffiecinfobase/index.html FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual http://www.ffiec.gov/bsa_aml_infobase/default.htm <i>Security and Confidentiality of Nonpublic Information</i> FRS: 12 CFR 216.3(n); FDIC: 12 CFR 332.3(n); NCUA: 12 CFR 716.3(q); OCC: 12 CFR 40.3(n); OTS: 12 CFR 573.3(n) Interagency Guidelines Establishing Security Standards FRS: 12 CFR 208, Appendix D-2 and 12 CFR 225, Appendix F; FDIC: 12 CFR 364, Appendix B; NCUA: 12 CFR 748, Appendix A; OCC CFR 30, Appendix B; OTS CFR 570, Appendix B
Legal and Compliance Risks	<i>Check Clearing for the 21st Century Act (Check 21 Act)</i> FFIEC Check 21 InfoBase -- http://www.ffiec.gov/exam/check_21 Reg. CC, UCC, Reg. J, Federal Reserve Operating Circulars, ECCHO Rules <i>Check Collection System vs. ACH Transaction</i> NACHA Rules, Reg E, 12 CFR 205 <i>Anti-Money Laundering/Suspicious Activity Regulation</i> Bank Secrecy Act (BSA); Office of Foreign Assets Control (OFAC) Requirements <i>Due Diligence for Foreign Accounts or High Risk Customer</i> USA PATRIOT Act 312, 31 CFR 103.176
Operational Risks	<i>Authentication Method for Customers</i> Interagency Guidance on Authentication in an Internet Banking Environment FRS: SR 05-19; FDIC: FIL 103-2005; NCUA: LTCU 05-CU-18; OCC: Bulletin 2006-35; OTS: CEO Memo 228 FFIEC IT Examination Handbook
Risk Management: Mitigation and Controls	<i>Risk Management of Remote Deposit Capture</i>
Customer Due Diligence and Suitability	<i>Risk Management of Remote Deposit Capture</i> USA PATRIOT Act Sections 312, 313 and 319(b) 31 CFR 103.175 -103.177, 103.185 FFIEC Bank Secrecy Act / Anti-Money Laundering Examination Manual, Refer to Foreign Correspondent Account Recordkeeping and Due Diligence section and the Correspondent Account (Foreign) section BSA/AML Manual Special Measures -- specific discussion of RDC risks and risk mitigation NACHA -- "Third-Party Senders & the ACH Network: An Implementation Guide"
Vendor Due Diligence and Suitability	<i>FFIEC IT Examination Handbook -- Outsourcing Technology Services Booklet</i>
RDC Training for Customers	<i>FFIEC Risk Management of Remote Deposit Capture</i> Customer Due Diligence, page 6
Contracts and Agreements	<i>FFIEC Risk Management of Remote Deposit Capture</i> FFIEC Risk Management of Remote Deposit Capture, page 6
Business Continuity	<i>FFIEC IT Examination Handbook -- Business Continuity Planning Booklet</i>
Other Mitigation & Control Considerations	<i>FFIEC IT Examination Handbook -- Operations Booklet</i>
Risk Management: Measuring and Monitoring	<i>FFIEC Risk Management of Remote Deposit Capture</i> Risk Management: Measuring and Monitoring, page 8

Risk Management: Risk Assessment

Publish Date: January 14, 2009

http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf

Page 1

Narrative: Remote Deposit Capture (RDC), a deposit transaction delivery system, allows a financial institution to receive digital information from deposit documents captured at remote locations. These locations may be the financial institution's branches, ATMs, domestic and foreign correspondents, or locations owned or controlled by commercial or retail customers of the financial institution. In substance, RDC is similar to traditional deposit delivery systems at financial institutions; however, it enables customers of financial institutions to deposit items electronically from remote locations. RDC can decrease processing costs, support new and existing banking products, and improve customers' access to their deposits; however, it introduces additional risks to those typically inherent in traditional deposit delivery systems.

This guidance addresses the necessary elements of an RDC risk management process in an electronic environment, with emphasis on RDC deployed at a customer location. The general principles of RDC risk management discussed here are also applicable to financial institutions' internal deployment and other forms of electronic deposit delivery systems (e.g., mobile banking and automated clearing house [ACH] check conversions).

Also see:

FRS: 12 CFR 216.3(n)

FDIC: 12 CFR 332.3(n)

NCUA: 12 CFR 716.3 (q)

OCC: 12 CFR 40.3 (n)

OTS: 12 CFR 573.3

FRS: 12 CFR 208, Appendix D-2 and 12 CFR 225, Appendix F

FIL-4-2009

OCC Interpretive Letter #1036

August 10, 2005

Interpretive Letter #1036, 12 USC 36

<http://www.occ.treas.gov/interp/aug05/int1036.pdf> (Accessed August 20, 2009)

Narrative: This letter was in response to a bank asking if a bank or branch license was necessary if the intended user was a customer and the location of the Remote Deposit Capture System was in the customer's office.

Conclusion

"Therefore, we conclude that a remote deposit capture terminal as described in your letter is a not branch within the meaning of the McFadden Act, even if such a terminal is established (owned or rented) by a national bank. If the terminal instead is owned or rented by the customer, then it still is not a branch because it is not established by a bank, whether it is considered to "receive deposits" or not. Since the terminal is not a branch, the customer's location where the terminal is deployed also is not a branch. Therefore, it does not matter for branching purposes where the electronic deposit is considered to be "made" or "received," and so we express no opinion on those questions."

Also see:

1. See, e.g., Bonnie McGeer, *Remote Deposit Boosts Service, Cuts Costs*, American Banker, Jan. 18, 2005

2. Pub. L. No. 108-100, 117 Stat. 1177 (2003), *codified at* 12 U.S.C. § 5001-5018. The Board of Governors of the Federal Reserve System has issued implementing regulations that are primarily codified as Subpart D of Regulation CC, 12 C.F.R. § 229.51 *et seq.*
3. The leading case explaining these terms is *Independent Bankers Ass'n of America v. Smith*, 534 F.2d 921 (D.C. Cir.), *cert. denied*, 429 U.S. 862 (1976)
4. 12 U.S.C. § 36(j)
5. 12 C.F.R. § 7.4003

Gramm, Leach, Bliley Act (GLBA) 501(b)

August 24, 2001

15 USC, Subchapter I, Sec. 6801-6809

<http://www.ftc.gov/privacy/glbact/glbsub1.htm>

Narrative: The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), protects the privacy of consumer information held by financial institutions and requires financial institutions and their affiliates to give consumers privacy notices that explain the institutions' information sharing practices. The Act also provides consumers with the right to limit some sharing of their information.

Section 501 (b) of GLBA requires financial institutions to implement comprehensive security measures that protects the confidentiality of non-public information (customer information); protect against any anticipated threats or hazards to the security or integrity of such information and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

This section also requires vendors of financial institutions that provide products or services that could expose them to non-public information in the institution to sign an agreement to maintain processes and procedures to ensure customer information is kept safe.

However, if a financial institution, or a contracted vendor, knows or has a suspicion of a security breach—the financial institution must notify each customer that may be affected by the breach.

RISK MANAGEMENT: MITIGATION AND CONTROLS

FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual

August 24, 2007

http://www.ffiec.gov/bsa_aml_infobase/default.htm

Narrative: This manual provides guidance on identifying and controlling risks associated with money laundering and terrorist financing. The manual also contains an overview of BSA/AML compliance program requirements, BSA/AML risks and risk management expectations, industry sound practices, and examination procedures.

Also see:

31 CFR 103.36

FFIEC IT Exam: Operations Booklet

Sections 312, 313 and 319(b)

FFIEC Exam: Continuity Planning

31 CFR 103.177, 185, Section 311

Correspondent Account (Foreign section)

FFIEC Outsource Technology Services Booklet

Foreign Correspondence Account Recording and Due Diligence section

BSA/AML Manual Special Measures-specific discussion of RDC risks and risk management

USA Patriot Act 312, 31 CFR 103.176

USA Patriot Act Amendments to BSA

FFIEC IT Examination Handbooks

What is the InfoBase?

Narrative: The FFIEC InfoBase" concept was developed by the Task Force on Examiner Education to provide field examiners in financial institution regulatory agencies with a quick source of introductory training and basic information. The long-term goal of the InfoBase is to provide just-in-time training for new regulations and for other topics of specific concern to examiners in FFIEC's five member agencies.

The Federal Financial Institution Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS). Visit the Council's website for press releases and information on the mission and work of the Council at <http://www.ffiec.gov/>.

The FFIEC Examiner Education Office created the FFIEC InfoBase, which is a vehicle that enables prompt delivery of introductory, reference, and educational training material on specific topics of interest to field examiners from the FFIEC member agencies. The IT Handbooks are updated and maintained electronically using the InfoBase vehicle.

What can be found on the InfoBase?

The following provides an overview of information in this InfoBase:

- The IT Booklets page allows access to all resources associated with individual FFIEC IT Examination Handbook booklets
- The Resources page provides a list of resources related to the booklet topics. Many of the listed documents can also be accessed directly from the Resources Page
- The Reference Materials page contains topical materials that supplement booklet content. The materials are provided for informational purposes, only. Disclaimer
- The Presentations page provides access to audio and printed versions of presentations, one general presentation on the IT Handbook revision process, and an introductory presentation on each IT Examination Booklet
- The Glossary is a master list of the glossary terms from each published booklet
- The Help section is where you can find assistance on using this website and the tools required to view any of the site content
- The Search function provides the ability to query the database for specific words. The search result will list all occurrences, by document
- The What's New section is where all recent changes to the InfoBase are listed. A brief description and the effective date for each change are included.

Source: <http://ithandbook.ffiec.gov/>

Interagency Guidelines Establishing Information Security Standards – Small-Entity Compliance Guide

January 14, 2009

Financial Institution Letter, FIL-4-2009

FRS: 12 CFR 208 Appendix D-2

<http://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010813/>

Narrative: The Federal Financial Institutions Examination Council has issued the attached guidance, "Risk Management of Remote Deposit Capture," to assist financial institutions in identifying risks in their remote deposit capture (RDC) systems and evaluating the adequacy of controls and applicable risk management practices. The guidance addresses the necessary elements of an RDC risk management process - risk identification, assessment, and mitigation - and the measurement and monitoring of residual risk exposure. The guidance also discusses the responsibilities of the board of directors and senior management in overseeing the development, implementation, and ongoing operation of RDC.

Federal Reserve and Treasury Department Announce Final Rule on Merchant Banking Activities

February 15, 2001

FRS: CFR 225, Appendix F

<http://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010813/>

Narrative: The rule implements provisions of the GLBA. The Board and the Secretary believe it permits a "two-way street" between securities firms and banking organizations while, at the same time, giving effect to statutory limitations and framework adopted by Congress to help maintain the separation of banking and commerce and ensure the safety and soundness of depository institutions.

FDIC Law, Regulations, Related Act

2000

FDIC: 12 CFR 364, Appendix B

Interagency Guidelines Establishing Information Security Standards

<http://www.fdic.gov/regulations/laws/rules/2000-8660.html>

Narrative: These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Guidelines also address standards with respect to the proper disposal of consumer information.

NCUA Record Retention

March 15, 2007

NCUA 12 CFR 749, Appendix A

RECORDS PRESERVATION PROGRAM AND RECORD RETENTION APPENDIX

<http://www.ncua.gov/regulationsopinionslaws/comment/750-RecPress/750-RecPreshtm>

Narrative: Credit unions often look to NCUA for guidance on the appropriate length of time to retain various types of operational records. NCUA does not regulate in this area, but as an aid to credit unions it is publishing this appendix of suggested guidelines for record retention. NCUA recognizes that credit unions must strike a balance between the competing demands of space, resource allocation and the desire to retain all the records that they may need to conduct their business successfully. Efficiency requires that all records that are no longer useful be discarded, just as both efficiency and safety require that useful records be preserved and kept readily available

Interagency Guidelines Establishing Standards for Safeguarding Customer Information

March 5, 2001

OCC CFR 30, Appendix B

<http://www.occ.treas.gov/fr/cfrparts/12CFR30.htm>

Narrative: The final rule of “Interagency Guidelines Establishing Standards for Safeguarding Customer Information; added Appendix B and removed Appendix C. Standards set forth apply to uninsured national banks, federal branches and federal agencies of foreign banks, and the subsidiaries of any national bank, federal agency of a foreign bank (except brokers, dealers, persons providing insurance, investment companies and investment advisers).

Legal and Compliance Risks

Check Clearing for the 21st Century ACT (Check 21 Act)

October 28, 2003

Public Law 108-100 October 28, 2003, H.R. 1474, 117 STAT. 1177 – 117 STAT. 1194

http://frwebgate.access.gpo.gov/cgi-in/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ100.108

Narrative: To facilitate check truncation by authorizing substitute checks, to foster innovation in the check collection system without mandating receipt of checks in electronic form, and to improve the overall efficiency of the Nation’s payment system and for other purposes.

FFIEC Check 21 InfoBase

October 28, 2003

Check Clearing for the 21st Century Act – Compliance Information for Examiners and Industry

<http://www.ffiec.gov/exam/check21/>

Narrative: The InfoBase contains a training presentation that provides concise overview for implementing regulation, an example of check processing under Check 21 consumer compliance and other requirements and an example concept for consumer compliance issues.

Also see:

Reg. CC Federal Reservations Operating Circulars

UCC ECCHO Rules

Reg J

Automated Clearing House (ACH) Check Conversion

March 5, 2007

Check Collection System vs. ACH Transaction

<http://www.electronicpayments.org/pdfs/arcwhitepaper.pdf>

Narrative: This document was written for individuals or organizations that want to know more about ACH check conversion, including BOC, the newest conversion application. The document provides a historical and legal overview of the ACH network, the impact and the use of the ACH network applications by consumers, specific details about the check conversion process and a comparison between check conversion and the recent Check Clearing for the 21st Century (referred to as Check 21).

Regulation E

March 9, 2009

Reg E, 12 CFR 205

http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title12/12cfr205_mai...

Narrative: This part carries out the purposes of the Electronic Fund Transfer Act, which establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. The primary objective of the act is the protection of individual consumers engaging in electronic funds transfers.

Also see:

Title 12—Banks and Banking

Chapter II—Federal Reserve System

Subchapter A-Board of Governors of the Federal Reserve System

Part 205—Electronic Fund Transfers (Regulation E)

USA Patriot Act

October 6, 2001

Public Law 107 – 56 – Oct. 26 2001, 107th Congress, H.R.3162

United and Strengthen America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

http://fincen.gov/statutes_regs/patriot/index.html

Narrative: The USA PATRIOT Act requires U.S. financial institutions to perform due diligence and, in some cases, enhanced due diligence, with regard to correspondent accounts established or maintained for foreign financial institutions and private banking accounts established or maintained for non-U.S. persons. The final rule issued today implements the general due diligence requirements pertaining to foreign financial institutions as well as the due diligence and enhanced scrutiny requirements pertaining to private banking accounts.

The notice of proposed rulemaking addresses the enhanced due diligence requirements pertaining to correspondent accounts maintained for certain foreign banks.

Also see:

USA Patriot Act 312

Interagency Guidance on Authentication in an Internet Banking Environment

October 13, 2005

FRS: SR 05-19

<http://www.federalreserve.gov/boarddocs/SRLETTERS/2005/sr0519.htm>

Narrative: The Federal Financial Institutions Examination Council (FFIEC) has issued the attached guidance titled *Authentication in an Internet Banking Environment*. This guidance updates and replaces the FFIEC's *Authentication in an Electronic Banking Environment* issued in 2001 and specifically addresses the need for risk-based assessments, customer awareness, and security measures to reliably authenticate customers accessing financial institutions' Internet-based services. The guidance also emphasizes that the agencies consider single-factor authentication, if it is the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a technology service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Also see:

FDIC 102-2005

OCC: Bulletin 206-35

NCUA

CEO Memo

LTCU 05-CU-18

FFIEC IT Examination Handbook

Uniting and Strengthen America's Appropriate Tools Required to Intercept and Obstruct Terrorism

December 2008

USA Patriot Act Section 312, 313 & 319(6)

http://www.ffiec.gov/bsa_aml_infobase/default.htm

Narrative: Sec 312: -IN GENERAL- Each financial institution that establishes, maintains, administers, or manages a private banking account or a correspondent account in the United States for a non-United States person, including a foreign individual visiting the United States, or a representative of a non-United States person shall establish appropriate, specific, and, where necessary, enhanced, due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering through those accounts. Sec 313: -IN GENERAL- A financial institution described in subparagraphs (A) through (G) of section 5312(a)(2) (in this subsection referred to as a 'covered financial institution') shall not establish, maintain, administer, or manage a correspondent account in the United States for, or on behalf of, a foreign bank that does not have a physical presence in any country. SEC 319(6): Section deals with the forfeiture of funds in interbank accounts and the ability of Federal banking agencies to subpoena bank records or summons banking staff in order to gain access to bank records. It also gave U.S. courts the authority to order a convicted criminal to return property located abroad.

Also see:

31 CFR 103.177; 103.185, Section 311

NACHA: "Third-Party Senders & the ACH Network: An Implementation Guide"

RISK MANAGEMENT: MEASURING AND MONITORING

Supervision of Technology Service Providers

May 2003

http://www.ffiec.gov/ffiecinfobase/html_pages/tsp_book_frame.htm

Narrative: "The "Supervision of Technology Service Providers" booklet is one of a series of updates to the 1996 FFIEC Information Systems Examination Handbook and rescinds chapters 2–7 of that handbook. This booklet primarily governs the supervision of technology service providers (TSPs) and briefly summarizes the Federal Financial Institutions Examination Council (FFIEC) member agencies' (agencies) expectations of financial institutions in the oversight and management of their TSP relationships. This booklet outlines the agencies' risk-based supervision approach, the supervisory process, and the examination ratings used for information technology (IT) service providers."⁶⁶

⁶⁶ http://www.ffiec.gov/ffiecinfobase/html_pages/tsp_book_frame.htm (Accessed August 21, 2009)