CHECK 21, REMOTE DEPOSIT CAPTURE and CHECK FRAUD: Summary and Detailed Explanation

Check 21, Remote Deposit Capture and Check Fraud….in Layman's Terms

Check 21's Final Rule includes an "Indemnity" provision that seriously affects an organization's liability for check fraud, under certain conditions. Because this provision is buried on page 58 of 114 pages, few people are aware of it or understand its implications. Organizations that understand the Indemnity are often motivated to use high security checks. The following is a brief explanation of the Indemnity provision.

Check 21 gives financial institutions the right to convert the paper checks they receive into electronic images, to process those images for payment instead of the original paper checks, and to destroy those paper checks after an undefined period of time. If necessary, the paying bank or its processor can re-convert the electronic image into a paper document known as a "substitute check" or Image Replacement Document (IRD).

The right to convert the original check into an image raises the question, "What if a fraudulent or altered check is converted and then shredded?" The Indemnity provision addresses that question.

The Indemnity provision says that if a loss occurred because the paying bank received an electronic image or an IRD instead of the original check, an Indemnity claim can be filed against the bank that presented the substitute check to the paying bank IF two conditions are met.

First, the original paper check had to have security features that could not be seen in the electronic image or substitute check. These are features that "do not survive imaging" and include features such as a true watermark, thermochromatic ink, chemical sensitivity, etc. These are some of the best features to prevent check fraud.

Second, the dollar amount of the check had to be sufficiently high that the paying bank would have physically inspected the check for those security features to verify its authenticity, if it had received the original check instead of a substitute check or electronic image. This is known as the Sight Review process. Every bank sets its own Sight Review threshold. One bank might inspect every check over $5000, and a different bank might inspect every check over $25,000.

Both conditions must be met to make an Indemnity claim. The Indemnity is valid for one year from the date the injured party discovers the loss (not from when the check was written). Note that under the exact same fraudulent situation, if the original check did not have the proper security features, it would not qualify for the Indemnity.

How does this relate to Remote Deposit Capture? The party that converts the paper check into an electronic image "issues" the Indemnity. Under RDC, the bank authorizes its client to electronically image the checks, not the bank. The company scans the checks it would normally send to the bank for deposit, and then electronically transmits the check images to the bank for deposit/collection. The bank processes the images and sends them to the various paying banks for collection. After a period of time, in our opinion not less than 60 days, the company can destroy the original paper checks.

Under the Check 21 Indemnity provision, **the entity that originally converts the paper check into an electronic image provides the Indemnity.** While there are many benefits for using RDC, companies should understand the risks and weigh the benefits against those risks. One risk is the obligation of providing an Indemnity for at least one year against certain types of check fraud.

(For an in-depth article, read "Check 21, Remote Deposit Capture and Check Fraud", written by Frank Abagnale and Greg Litster, and reviewed by the Federal Reserve Board.)

CHECK 21, REMOTE DEPOSIT CAPTURE and CHECK FRAUD

Frank Abagnale
President, Abagnale and Associates
abagnale.com

Greg Litster
President, SAFEChecks
Canoga Park, CA
greg@safechecks.com

Check Clearing for the 21st Century Act, aka "Check 21" was passed unanimously by the House of Representatives and the Senate in October 2003. It was signed by President George W. Bush on October 28, 2003 and became effective October 28, 2004.

Check 21 allows banks to (1) convert original paper checks into electronic images; (2) truncate the original check; (3) process the images electronically; and (4) create "substitute checks" for delivery to banks that do not accept checks electronically. The legislation does not require a bank to create or accept an electronic check image, nor does it give an electronic image the legal equivalence of an original paper check. Check 21 does give legal equivalence to a "substitute check" that is properly prepared. A substitute check, also known as an image replacement document (IRD), is a new negotiable instrument that is a paper reproduction of an electronic image of an original paper check.

A substitute check must: (1) contain an image of the front and back of the original check; (2) bear a MICR line containing all the information of the original MICR line; (3) conform to industry standards for substitute checks; and (4) be suitable for automated processing just like the original check. To be the legal equivalent of the original check, the substitute check must also (1) accurately represent all the information on the front and back of the original check, and (2) bear a legend that states "This is a legal copy of your check. You can use it the same way you would use the original check." While Check 21 does not mandate that any check be imaged and truncated, all checks except checks drawn on foreign banks[1] are eligible to be truncated into images and reconverted[2] into substitute checks. Bank customers do not have the option to "opt out" of Check 21.

CHECK 21 CONVERSION vs ACH CONVERSION

A check truncated into an electronic image and reconverted into a substitute check is not the same thing as a check that is converted into an ACH debit. They are entirely different processing mechanisms and are governed by different rules. A substitute check is governed by the Check 21 Act and the Fed's Final Rule. A check converted into an ACH debit is governed by ACH rules.

---

[1] Federal Reserve Board's Final Rule issued July 26, 2004. See Pages 81-82 AAA.229.2(aaa).3 Substitute Check. Visit www.FraudTips.Net to download a copy of the Check Clearing for the 21st Century Act, aka Check 21, and the Federal Reserve Board's Final Rule governing Check 21.

[2] ibid. Page 11, Footnote 15. "Reconverting" is the statutory term and reflects the fact that the original check is converted to electronic form and then later reconverted back to a paper substitute check.

WARRANTIES AND INDEMNITY

Check 21 does not require a bank to convert and truncate paper checks. It is entirely voluntary. A bank that chooses to convert a paper check into an electronic image that can then be reconverted into a paper substitute check provides two warranties and an indemnity that travel with each substitute check. Companies that convert checks using Remote Deposit Capture may bear the identical risks as banks that convert checks. The two warranties are (1) that the substitute check is properly prepared as described in the paragraph above, and (2) that no bank will be asked to make payment on a check that has already paid (no double debit).

Regarding the indemnity, the Final Rule states a bank "that transfers, presents, or returns a substitute check…shall indemnify the recipient and any subsequent recipient…for any loss incurred by any recipient of a substitute check if that loss occurred due to the receipt of a substitute check instead of the original check."[3] It goes on to say that if a loss "…results in whole or in part from the indemnified party's negligence or failure to act in good faith, then the indemnity amount …shall be reduced in proportion to the amount of negligence or bad faith attributable to the indemnified party." [4]

The Fed gives this example.

"A paying bank makes payment based on a substitute check that was derived from a fraudulent original cashier's check. The amount and other characteristics of the original cashier's check are such that, had the original check been presented instead, the paying bank would have inspected the original check for security features and likely would have detected the fraud and returned the original check before its midnight deadline. The security features that the bank would have inspected were security features that did not survive the imaging process. Under these circumstances, the paying bank could assert an indemnity claim against the bank that presented the substitute check.

"By contrast with the previous example, the indemnity would not apply if the characteristics of the presented substitute check were such that the bank's security policies and procedures would not have detected the fraud even if the original had been presented. For example, if the check was under the threshold amount the bank has established for examining security features, the bank likely would not have caught the error and accordingly would have suffered a loss even if it had received the original check."[5]

The indemnity does not cover a loss that is not directly attributable to the paying bank receiving a substitute check instead of the original check.

The warranties and indemnity are very powerful, and give companies and paying banks a clear defensive strategy against losses that result directly from receiving a substitute check instead of an original paper check. It may also deter banks and companies from truncating high-dollar checks because the warranties and indemnity provided by the truncating party continue for one year beyond the date the injured party first learns of the loss. The Final Rule is clear that a "…claim shall be brought within one year of the date on which the person's cause of action accrues. …a cause of action accrues as of the date on which the

[3] ibid. Page 58, Substitute Check Indemnity

[4] ibid. Page 59, Comparative Negligence

[5] ibid., pages 99-100, Substitute Check Indemnity

injured person first learns, or by which such person reasonably should have learned, of the facts and circumstances giving rise to the cause of action, including the identity of the warranting or indemnifying bank against which the action is brought." [6]

It is important to note that the one-year timeframe begins when the injured party learns or should have learned of the loss, not when the loss actually occurred. Thus, the actual risk tail to the converting bank or company is greater than one year.

REMOTE DEPOSIT CAPTURE

Remote Deposit Capture is a service offered by many financial institutions that uses new technology to speed up a company's depositing process. Using a desktop scanner in its office, a company truncates the checks it normally would send to the bank for deposit. The company transmits the file of check images to its bank, which in this scenario would be the "truncating bank" (see § 229.2(eee) of Regulation CC and its commentary). The bank processes the file and sends the images of the checks for collection to their respective banks. The images are either presented for payment electronically or as substitute checks.

While the technology is exciting, Remote Deposit Capture is not without financial risk. First, depending on the company's agreement with its bank, the company may need to store the original check in a secure location for a period of time in case it is needed. Second, and more importantly, by their agreements truncating banks are likely to "pass back" liability for Check 21-related losses to their image-depositing customers who choose to deposit check images. The statute of limitations in the law for these types of losses is one year after the cause of action accrues. The cause of action accrues as of the date the injured party learns, or reasonably should have learned, of the loss.

INDEMNITY CLAIMS

In an indemnity claim, a party receiving a substitute check – for example, the paying bank – claims that it has incurred a loss attributable to receiving a substitute check in place of the original check. The paying bank would bring such claim against the reconverting bank, i.e., the bank that created the substitute check. Typically, in turn, reconverting banks have agreements in place with the upstream banks from which they receive electronic check files, such that they can recover from these banks, i.e., a reconverting bank typically has agreements in place such that it can recover from the truncating bank.[7] And, as mentioned in the previous paragraph, truncating banks typically have agreements in place with their remote-capture depositors such that they can recover from those depositors.

Examining a check for security features before its truncation (e.g., at the point of sale or deposit preparation) cannot prevent a Check 21-related indemnity claim because the party (person or company or bank) truncating the check likely has no knowledge of the security

[6] ibid. Page 67(c) Jurisdiction.

[7] For example, Regulation J functions as this agreement for the Reserve Banks when the Reserve Banks act as reconverting bank. If (1) a bank – the truncating bank – deposits checks electronically with the Reserve Banks, (2) the Reserve Banks create a substitute check for presentment to the paying bank, and (3) the paying bank that receives the substitute check brings a Check 21 claim against the Reserve Banks, Regulation J enables the Reserve Banks to recover on that Check 21 claim from the truncating bank.

features contained in an authentic check drawn on the account in question.[8] That is to say, checks truncated under the authority provided by Check 21, whether truncated by a bank or by a bank's customer using remote deposit capture, are typically truncated without knowing whether the loss of security features existing in the original check stock due to truncation will later result in an indemnity claim brought by the paying bank on the basis of damages that it would have been able to prevent had it been presented with the original check.

Moreover, if a counterfeit original check is truncated at the point of sale or in deposit preparation, the absence of security features in that counterfeit original check (i.e., the absence of the security features present in an authentic original check drawn on the account in question) would *not* prevent an indemnity claim by a paying bank that receives that check in substitute check form. The paying bank's argument would be that it would have inspected the counterfeit original check for security features, found them to be absent, and returned the check unpaid, and that it therefore incurred a loss due to having been presented with a substitute check in lieu of the (counterfeit) original check.[9]
If a loss results from a truncated item drawn on an account that uses original checks with non-image-survivable security features, AND if the dollar amount of the item was sufficiently high that the paying bank would have examined the check for those security features when it was presented for payment, the party that truncated the check may be face an indemnity claim. On the other hand, if the authentic check does not contain image-survivable security features, OR if the dollar amount is so low that the paying bank would not have examined the check when it was presented for payment, there are no grounds for an indemnity claim.

From a liability and risk aversion viewpoint, the safest checks to truncate are small-dollar items; the riskiest are larger-dollar items because 1) higher-dollar checks are more likely to be physically inspected by the paying bank; and 2) companies and individuals that issue higher-dollar checks are more likely to use high-security checks with features that do not survive imaging.

A company or individual that elects to use checks with security features that do not survive the image conversion process may be better off in a Check 21 world. This is especially true for account holders that issue higher-dollar checks, and for banks with a lower sight review threshold. In today's Check 21 world, a bank's most prudent risk-aversion strategy would be to encourage its customers to use high security checks with security features that do not survive imaging, and to lower its sight review threshold. Moreover, banks that offer Remote Deposit Capture capabilities would be wise to fully disclose the associated risks to their customers.

---

[8] Examining a check for security features may matter in a Holder in Due Course lawsuit. If a check is accepted as payment for goods or services, and the face of the check has a warning band that describes specific security features that one should look for to authenticate the check, if the recipient fails to examine the check for those security features, the recipient may be barred from seeking Holder in Due Course status if the check is returned unpaid. Visit www.FraudTips.net/holder. Click on Holder In Due Course and Check Fraud.

[9] It is not necessary for there to be a Check 21 warranty claim in order for the paying bank to bring a Check 21 indemnity claim. The truncating bank and/or its remote-deposit-capture customer may be liable for a Check 21 indemnity claim even if the substitute check in question bears a good image and is a legal equivalent of the original check. For more detail in this regard, see the last paragraph on page 9 of this Federal Reserve Board document:
http://www.federalreserve.gov/boarddocs/press/bcreg/2004/20041022/attachment.pdf.

CHECK SAFETY FEATURES

The two primary purposes for using many safety features[10] in checks are (1) to authenticate an original document, and (2) to deter criminal activity by thwarting their different methods used to alter or replicate checks. The minimum number of safety features a check should have is eight, and more is better. Among the best safety features are fourdrinier (true) watermarks in the paper, thermochromatic ink, and paper or ink that is reactive to at least 15 chemicals. These safety features cannot be imaged and replicated, which, in an age of desktop publishing, is why they are the best.

In addition to their fraud-deterrent value, when an individual or organization uses high security checks that include safety features that do not survive the image conversion process, they position their bank for an indemnity claim against the presenting bank. The presenting bank passes the indemnity claim upstream, ultimately back to the original truncating bank or company. This assumes that, in addition to the customer using high security checks, the paying bank has a sight review threshold such that the original check would have been examined had it been presented, a critical element in an indemnity claim.

Because of the risk associated with the indemnity, the largest banks in America have actively looked for check safety features that will survive the imaging process while still being useful, ie. not replicable by forgers. By their very nature, image-survivable security features can be replicated with a color copier or scanner. According to Frank Abagnale and The Standard Register Company, there are no check safety features that are image survivable that are useful.[11] A security feature called "Secure Seal," which is a type of bar code with encrypted check data and is usually laser printed, is image survivable and is useful. Contact Greg Litster for information on Secure Seal.

CHECK 21 FRAUD PREVENTION STRATEGIES

In a Check 21 world, the defensive strategies are straightforward:

(1) Every bank should offer Positive Pay at an affordable price, and every company, municipality and organization should use the service. Most banks charge for Positive Pay; any company deterred by the price should consider the fee an insurance premium that is far less expensive than attorney fees or a check fraud loss. For useful information about Positive Pay, on the Web visit PositivePay.net and SafePay123.com.

(2) Make large dollar payments electronically.

(3) Every company, municipality and individual should use high security checks with 10 or more safety features. The checks should include a true watermark, thermochromatic ink and be reactive to at least 15 chemicals. **SAFEChecks**, the **Supercheck** (for consumers) and the **SuperBusinessCheck** are high security checks that were designed by Frank Abagnale with these and many additional features so individuals, organizations, companies and municipalities could enjoy maximum security with a controlled, reasonably priced check. SAFEChecks and the Supercheck have 12

---

[10] Frank Abagnale publishes an 18-page color brochure titled *Check Fraud, Holder in Due Course, Check 21 and Identity Theft*. Check security features are discussed in detail and are shown in color. It is available without charge through his office or through SafeChecks. Call (800) 755-2265 ext. 3304.

[11] A white paper titled "Check 21 and Image Security" by Frank Abagnale and The Standard Register Company can be downloaded at www.FraudTips.Net. Click on Check 21.

security features, and the SuperBusinessCheck has 15. Call (800) 755-2265 ext. 3309 to request samples, or visit Supercheck.net and SafeChecks.com

(4) Avoid using laser checks that can be purchased entirely blank by multiple organizations and people because the stock is not controlled.

(5) Banks and their service providers should lower their sight review thresholds and re-train inspectors to look for physical security features. In light of the indemnity provision of Check 21, it would behoove banks to encourage their customers to use high security checks along with Positive Pay.

About the authors

Frank Abagnale is one of the world's most respected authorities on the subject of forgery, secure documents, identity theft and embezzlement. For over 30 years he has lectured to and consulted with hundreds of financial institutions, corporations and government agencies around the world, including the FBI. More than 14,000 financial institutions, corporations, and law enforcement agencies use his fraud prevention materials. He is the author and subject of *Catch Me If You Can*, a Steven Spielberg movie that starred Tom Hanks and Leonardo DiCaprio. Mr. Abagnale can be contacted at (800) 237-7443.

Greg Litster is president of SAFEChecks, and a former 18-year banker. He is an associate of Frank Abagnale, and is publisher and editor of Mr. Abagnale's publication, ***The Fraud Bulletin***. It can be downloaded at safechecks.com/bulletin.htm. SAFEChecks sells high security checks, secure check printing software, and Positive Pay file formatting software. Mr. Litster lectures on fraud prevention across the United States, and provides expert witness services in fraud cases both nationally and internationally. He can be contacted at greg@safechecks.com or by phone at (800) 949-2265.

Disclaimer

****

The **Abagnale SuperBusinessCheck** has 16 security features and **SAFEChecks** have 12 security features, including heat sensitive ink, a true watermark and properly worded warning bands. Both are strictly controlled, high security check stock that were designed by Frank Abagnale, one of the world's foremost authorities on fraud prevention. Both are manufactured and sold by SAFEChecks.

www.safechecks.com