CHECK 21, REMOTE DEPOSIT CAPTURE and CHECK FRAUD

Frank Abagnale
President, Abagnale & Associates
abagnale.com

Greg Litster
President, SAFEChecks
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.

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 and individuals that convert checks using a Remote Deposit Capture device 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 debits).

---

[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.

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 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

Most financial institutions allow their customers to deposit checks remotely ("Remote Deposit Capture") via a smart phone app or a desktop scanner. The check images captured by those devices are uploaded to the bank, which in this scenario would be the "truncating bank" (see § 229.2(eee) of Regulation CC and its commentary). The bank processes the uploaded file and sends those check images for collection to their respective banks. The images are presented for payment electronically or as substitute checks.

---

[3] ibid. Page 58, Substitute Check Indemnity

[4] ibid. Page 59, Comparative Negligence

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

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

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.

MOBILE REMOTE DEPOSIT CAPTURE

The advent of mobile banking was unforeseen in 2003 when Congress passed Check 21; its inevitable evil twin, mobile banking fraud, was also unforeseen. However, the Check 21 rules apply equally to mobile banking.

Because depositing checks via a smart device (Mobile Remote Deposit Capture, aka mRDC) is highly popular, almost all banks offer mRDC. Fraudsters haven't directly targeted mRDC users' devices on a large scale; however, cases of dishonest mobile users purposely double-depositing the same check at multiple banks, or cashing the check at a check cashing store after depositing via a smart phone, are growing dramatically.

The Federal Reserve Board predicts that almost half of all mobile users will adopt mobile banking in one capacity or another. It behooves all mobile phone users and financial institutions alike to be alert and vigilant toward fraud prevention.

MOBILE DEPOSITS & DUPLICATE PRESENTMENTS

The legal basis for creating and depositing a digital image of a check is Check 21. Check 21 has a rule ("Warranty") that specifically prohibits a check or its image from being presented for payment more than once. Check 21 provides a powerful recovery remedy if this occurs.

Consider this example: Dishonest Don receives a check and deposits the check (its electronic image) via his bank's smart phone app. He still has the physical paper check, which he later cashes at a check cashing store. When the check cashing store deposits the original paper check and its image is presented to the drawer's bank for payment, **its second presentment breaches the Warranty** made by Dishonest Don when he deposited the check via his smart phone app. When he downloaded the app, Dishonest Don clicked a box agreeing to the terms of using the app. Banks' terms include that the user WILL NOT deposit or cash a check that was deposited using the mobile banking app.

Under Check 21, because of the second presentment, the first check (deposited via the bank app) can be charged back to the bank of first deposit (BOFD) under a Breach of Warranty claim for up to one year from the date the injured party **discovers the loss**, even if the loss was not discovered for months or even years.[7]

[7] In a check cashing store scenario, the check cashing store is the "injured party" due to the returned check. The check cashing store is also a holder in due course (HIDC). A HIDC can sue the drawer (maker) of the check for three (3) years from the date the check was returned. When a check cashing store goes after the drawer, it gives the drawer "notice." That likely would be the first time the drawer would have "reason to know" about the duplicate presentment, AND is Day One of the one-year period to return the first presentment to the bank of first deposit. **Note**: The drawer, after being sued or otherwise notified, is not yet an "injured party" for Check 21's Breach of Warranty claim purposes. Only when the drawer actually pays the check casher does the drawer convert from being a witness to becoming the injured party, the victim. Suing/contacting the drawer (in writing, as "evidence") also gives the drawer "notice" of the duplicate presentment. The drawer then has up to One Year from that date to file a Breach of Warranty claim with its bank. The drawer's bank will file a Breach of Warranty claim against the bank of first deposit (BOFD). The BOFD has no legal options except to pay the face value of the check and any associated costs, such as the returned check fee, and perhaps any legal expenses.

MOBILE DEPOSITS AND HOLDER IN DUE COURSE

There are additional fraud protections offered by the Check 21 Rules. Consider this scenario: John Doe picks up a check made payable to "John Doe" from a business or individual. He walks outside and deposits the check remotely using his smart phone. He then walks back inside and returns the check, asking that it be replaced with a new check made payable to John Doe OR Jane Doe. The issuing person or company reissues a new check payable to John Doe or Jane Doe. They don't place a Stop Payment on the first check because it is in their possession.

John Doe quickly cashes the second check, and waits overnight for the first check to clear before withdrawing the money from the first check. Unfortunately, the drawer issuing the check can be held liable for both checks. This is because the second check was cashed at the bank, and the first check was deposited remotely. While banks often cooperate to stop fraudulent activity, John Doe's bank is a Holder In Due Course and has no obligation to return the funds to the issuer.

To prevent this kind of theft, if a check leaves your possession for any length of time and is returned for a replacement check, place a Stop Payment on the check (even though HIDC trumps a Stop Payment). Require the recipient to sign an affidavit declaring the check was not deposited remotely, and that the recipient has no claim to those funds, and accepts responsibility for all expenses to recover those funds.

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.[8] 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 truncating the check (person or company or bank) likely has no knowledge of the security features contained in an authentic check drawn on the account in question.[9] 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.

---

[8] 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.

[9] 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.

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.[10]

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 chooses 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 limits. 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 dollar threshold. Moreover, banks that offer Remote Deposit Capture capabilities would be wise to fully disclose the associated risks to their customers.

CHECK SAFETY FEATURES

The two primary purposes for using many safety features[11] 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, heat-sensitive 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. Using a "controlled" check stock that includes these features is critically important. ("Controlled" means that the identical check stock is not available completely blank to other organizations – or criminals.)

In addition to their fraud-deterrent value, when an individual or organization uses high security checks that include safety features that don't 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 the customer uses high security checks and the paying bank has a sight review threshold such that the original check would have been examined had it been presented. Both are critical elements in an Indemnity Provision claim.

---

[10] 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.

[11] Frank Abagnale publishes a 32-page color brochure titled *The Fraud Bulletin, Volume 17*. 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.

SECURE BARCODE

Because of the risk associated with Check 21's Indemnity provision, the largest banks in America have actively looked for check safety features that will survive the imaging process while still being useful, i.e. not replicable by forgers. By their very nature, image-survivable security features can be replicated with a color copier or scanner.

There is a relatively new security feature called "**secure barcode**." This is an encrypted barcode that is printed on the face of a laser check when a check is being printed on a laser printer. The secure barcode is essentially an "onboard" Payee Positive Pay file for that specific check. The secure barcode contains all of the check data that is printed on the check, including the check number, account number, payee name, dollar amount, date and time the check was printed. The barcode is image survivable when the paper check is converted into a digital image (X-9 file).

Contact Greg Litster for information on the secure barcode: Greg@SAFEChecks.com.

CHECK 21 FRAUD PREVENTION STRATEGIES

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

(1) Every bank should offer Payee Positive Pay at an affordable price, and every company, municipality and organization should use the service. (Payee Positive Pay is superior because Positive Pay does not match on the payee name.) Most banks charge for Positive Pay services; an organization deterred by price should consider the fee as an insurance premium that is far less expensive than attorney fees or a check fraud loss. For useful information about Positive Pay, visit PositivePay.net.

(2) Use Dual Authorization Control when making electronic payments. DAC: One group of people originate and send the payment to the bank, but that payment is held by the bank until a second group of people log in to review the payment and release it. This is the only way to beat hackers!

(3) Make large dollar payments electronically ONLY after confirming with complete certainty that the account the funds are being sent to belongs to the intended recipient and not to a fraudster who sent in a bogus change-of-bank and remittance notification.

RECOMMENDATIONS

Every company, municipality and consumer/individual should use high security checks with 10 or more safety features. Checks should include a true watermark, thermochromatic ink, and be **permanently reactive** to at least 15 chemicals.

Checks designed by Frank Abagnale, specifically, the **SuperBusinessCheck**, the **Supercheck** (for consumers), and the original **SAFECheck** are high security checks containing these and additional security features. Individuals, organizations, companies and municipalities could enjoy maximum security with a highly secure, controlled, reasonably priced check.

Since its founding in 1996, SAFEChecks has NEVER had a check replicated or used in a check fraud scam.

(1) ***SAFEChecks*** and the ***Supercheck*** have 12 **useful** security features; the ***SuperBusinessCheck*** has 16 **useful** features. Call (800) 755-2265 to request check samples. Visit SAFEChecks.com

(2) Avoid using laser checks that can be purchased entirely blank because fraudsters buy the same check stock, and scan and create counterfeit checks that look completely genuine.

(3) Banks and their service providers should **lower Sight Review $$ thresholds** & re-train inspectors to look for physical security features. Email info@SAFEChecks.com for an 18-page document titled

Check 21, Remote Deposit Capture and Check Fraud – The Indemnity Provision

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 a substitute check (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 must have contained security features that are not visible in the electronic image or substitute check. These features "do not survive imaging," such as a true or artificial watermark, thermochromatic ink, chemical sensitivity, etc. These are some of the best features to prevent check fraud via counterfeit checks.

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 — as if had it received the original check instead of a substitute check or electronic image. This is the "Sight Review" process, and every bank sets its own Sight Review threshold: A small bank might inspect every check over $2000 while a different bank might inspect checks over $20,000. Keep the $$ threshold **very low** to trigger the Indemnity.

Both conditions must be met to assert an Indemnity claim. An Indemnity claim can be made for one year from the date the injured party discovers the loss (not when the check was paid). Note: Under an identical fraudulent situation, if the original check did not have the proper security features, it would not qualify for the Indemnity claim.

How does this relate to Remote Deposit Capture (RDC)? The party that converts the paper check into an electronic image provides the Indemnity. Under RDC, the bank authorizes its client to electronically image the checks instead of sending them to the bank. The company scans the checks that would normally be sent to the bank for deposit, and then electronically transmits the check images to the bank for deposit.

The process is similar under Mobile Remote Deposit Capture (mRDC), with the individual taking a picture of the check with a mobile device and app, and transmitting the check image to the bank for deposit. The bank processes those images and sends them to the Fed or various paying banks for collection. After a period of time (we recommend not less than 60 days) the company or person can destroy the original paper checks.

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 46 years Mr. Abagnale has advised 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 film that starred Tom Hanks and Leonardo DiCaprio.

For information about Mr. Abagnale, please visit https://abagnale.com/. Scroll down on his Home page.

Greg Litster is president of SAFEChecks, and a former 18-year banker. As Senior Vice President he oversaw Cash Management, Title/Escrow and Correspondent Banking. Mr. Litster is co-editor and publisher of Mr. Abagnale's Fraud Bulletins. The most recent Fraud Bulletin and prior versions can be downloaded at https://www.safechecks.com/fraud-education/the-fraud-bulletin.php.

Mr. Litster lectures on check fraud, cybercrime and embezzlement, and provides expert witness services in check fraud, ACH/Wire fraud, & embezzlement cases. Contact: greg@safechecks.com or (800) 755-2265.

SAFEChecks sells **high security checks** designed by Frank Abagnale that **cannot** be chemically washed without leaving a permanent stain, and have never been replicated or used in a fraud scam in 30+ years.

SAFEChecks strongly endorses using Positive Pay with Payee Name match, and also offers software to create and send properly formatted check-issue files to the bank. https://www.safechecks.com.