Check 21 and Image Security

A review of the implications associated with identifying image-survivable security features in response to recent Check 21 legislation.

Revised 3/04

FRANK W. ABAGNALE
25 Years
SECURE DOCUMENT VERIFICATION MANUAL

Standard Register

Dan Thaxton
The Standard Register Company

Frank W. Abagnale
Secure Document Consultant

Executive Summary

This document offers a review of the implications associated with identifying image-survivable security features in response to recent Check 21 legislation.

CONCLUSIONS

While Check 21 will significantly speed the handling and collection of checks, the potential for enormous unprosecutable check fraud losses is nearly certain as the conversion process destroys the evidence of fraud in most cases. The indemnity required of the converting bank for a loss sustained by a paying bank because it received a substitute check rather than the original check with security features that did not survive the image conversion process will shift the liability for some losses to the converting bank.[1] For this reason, the search for effective image survivable security features is a high priority.

The "Holy Grail" of image-survivable security technology is a feature or features that could be authenticated using images already captured during the "normal" part of the sorting process. Unfortunately, this appears to be an unattainable goal. It is an understood rule that the resolution of copying equipment needs to be two times that of the original item to create an accurate reproduction. Since existing check readers can only "see" at resolutions approaching 240 dpi, they are inherently unable to distinguish between the appearance of an original item or a copy reproduced at 480 dpi or more. Most consumer-grade printers and copiers currently operate at 600 dpi or greater while commercial-grade machines can exceed 1200 dpi, creating a presumption that most copies will be of sufficient quality to be interpreted as original items on conventional read/sorters.

There still remains the possibility of an image-based solution. For example, those familiar with the copy VOID pantograph technology understand that it is possible to craft printed patterns that grow or shrink when they are viewed and/or reproduced by conventional technologies. It is believed that through the use of a series of specially designed patterns that either grow or shrink depending on the resolution of the reproduction equipment, it may be possible with sophisticated image processing software to differentiate between originals and mimics (ref U.S. patents 6.209.923 and US 6.394.358).

The key to a successful item protection process appears to remain where it has been in the past: at the point of entry. Any fraudulent item that enters into the payment system ultimately costs somebody. While the banks are seeking to improve their ability to identify a fraud with an image-survivable security feature, the only solution that protects both the banks and their customers is one that makes it possible to recognize a fake when it is presented. Absent national Positive Pay databases or comparable standards, points of acceptance continue to rely upon security devices that are difficult to mimic yet easy to recognize with the human eye, such as Thermochromic or OVI inks, watermarks, and evidence of tampering.

RECOMMENDATIONS

At this time there are no known image-survivable features that are fully effective. Financial Institutions and their service providers that choose to convert paper checks into electronic images do so at their own considerable risk and liability. While the risk of converting checks of $400 or less is small and may be tolerable, large dollar checks should not be converted. From a defensive position, companies and individuals should be encouraged by their financial institutions to use high security checks with eight or more security features, including true watermarks in the paper, thermochromatic inks, and chemically sensitive paper or ink to aid in the detection of fraud at the point of acceptance. Financial Institutions should offer such checks to their business and consumer customers.

Dan Thaxton	Frank W. Abagnale
Manager, Security Solutions	Secure Document Consultant
The Standard Register Company	Abagnale & Associates
8-Dec-03	

[1] Visit http://www.federalreserve.gov/BoardDocs/Press/bcreg/2003/20031222/attachment.pdf for the proposed rules governing Check 21 issued December 22, 2003. Read Page 76-77, Substitute Check Indemnity.

SUPPORTING DATA

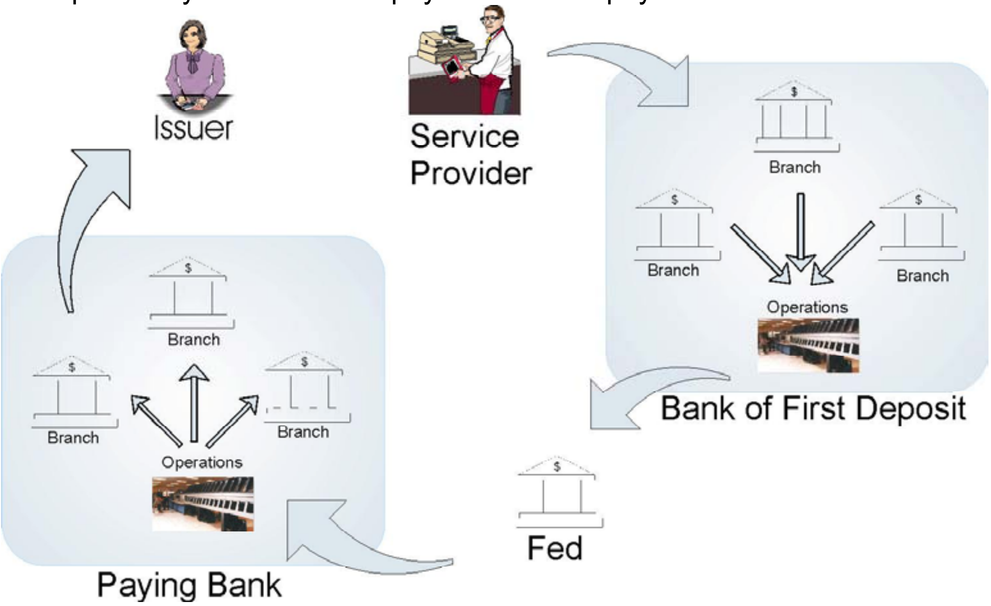
Brief Overview Of Check 21

Check Clearing for the 21st Century Act, the legislation known as Check 21, was signed into law by President George W. Bush on October 28, 2003 and goes into effect October 28, 2004. Check 21 allows for many things, including the right, but the not requirement, to convert a paper check into an electronic image (a substitute check) at any point in the clearing process. This substitute check is the legal equivalent of the original paper check. The proposed legislation requires that the converting entity or financial institution (often the bank of first deposit) provides warranties that the substitute check includes all the information contained on the original check, and that the substitute check is not processed for payment twice (no double debit). It also contains an indemnity that allows a paying bank to charge back a loss resulting from receiving a substitute check rather than the original check, after its midnight deadline. The indemnity requires that the original check have safety features that did not survive the image conversion process, and that the bank's procedures were such that it would have reviewed and likely caught the alteration or counterfeit had the original check been presented.

While Check 21 will significantly speed the handling and collection of checks, the potential for enormous un-prosecutable check fraud losses is nearly certain, as the conversion process destroys the evidence of fraud in most cases. The indemnity will shift the liability for losses away from the paying bank to the converting entity, with potentially devastating results to the converter. For this reason, the search for effective image-survivable security features is a high priority.

Legacy Payment Processing System

Prior to Check 21, the payment processing system involved a check being submitted for payment by an *issuer* to a *provider.* The *provider* submits the check to the *Bank of First Deposit* for payment into their account. The *Bank of First Deposit* processes the check and determines whether it is an *In House Item* (drawn against itself) or an external item that needs to be submitted elsewhere for payment. Items that are drawn against other institutions are forwarded for payment, sometimes directly but more often through the Federal Reserve. Under current law financial institutions have only a couple of days to submit the physical item for payment.



After the initial sorts, the *Paying Bank* sorts all items received from outside institutions and prior *In House* items again to establish which accounts the items are drawn against. Accounts are debited according to the items processed and payments are issued to the submitting institutions. Actual items are usually sorted down to the individual issuer's account and returned to the *issuer,* although many banks now eliminate the actual return of processed items.

Under Check 21, an electronic image of the item created by the *Bank of First Deposit* is now the only thing that needs to be forwarded to the *Paying Bank* for processing, eliminating the need to transport the physical item cross-country and re-sort it upon receipt at the paying bank.

Image-survivable Security

Image-survivable Security simply describes the security devices employed on an original item that bridge effectively into the electronic item. A robust image-survivable security technology would actually be capable of distinguishing an alteration or fake from an original item during the digitization process.

Ever since reader/sorters began capturing digital images of checks the banking industry has been interested in employing one or more image-survivable security features. Over the years a host of solutions have been proposed and marketed, including but not limited to: Angstrom and CheckSmart UV inks, Unisys and ChequeGard barcodes, PhotoSecure and Secure Products converting phosphors, and complex printed patterns or "digital watermarks" from companies like Digimark and Standard Register. Business forms printers like Standard Register have explored and/or marketed several of the solutions noted. While diverse in the technologies employed to deliver security, all of the solutions noted above employ some special capability that can be identified and authenticated mechanically with the aid of hardware detection and/or software interpretation of the captured image during or following the read/sort process. In general, all image-survivable security solutions can be broken into two key categories: those that need additional hardware to complement the image capture process, and those that utilize existing image capture hardware to determine authenticity.

Add-On Technologies

Add-on technologies require some modification to the reader/sorter hardware to facilitate recognition of the additional security device. Add-on technologies usually involve printing marks and codes using Ultra-Violet inks or converting phosphors (inks that absorb energy at one frequency and reflect it at another) and using a special reader to activate and "see" the expected patterns.

Add-on technologies have the advantage of being direct and effective in their implementation. Unfortunately, the costs of printing these marks, as well as modifying and integrating the necessary authenticating equipment into the reader/sorter hardware has been prohibitive to date. For example, one of the more "complete" add-on solutions was a converting phosphor marketed by an East Coast concern. This mark required a license of approx a half penny per item to produce, as well as a significant (5 figure) per-unit annual lease of the detection equipment on an IBM 3890 family sorter. One of the unique aspects of this solution was that it had IBM's cooperation in integrating the detection hardware into their 3890's. But, while this solution was marketable and actually field tested, overall program costs were too prohibitive for the financial institutions or their commercial accounts to absorb and the product eventually died.

Developing detection equipment that integrates seamlessly with the four major read/sorter vendors is no small challenge, especially when these vendors have intentionally differentiated themselves to define a competitive position.

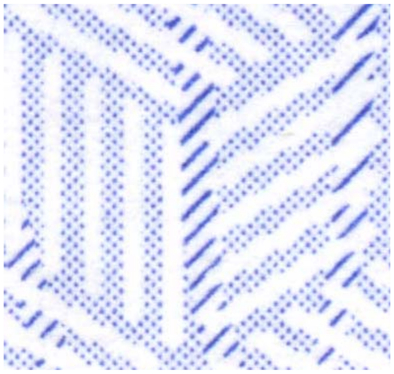
Existing Tie-Ins

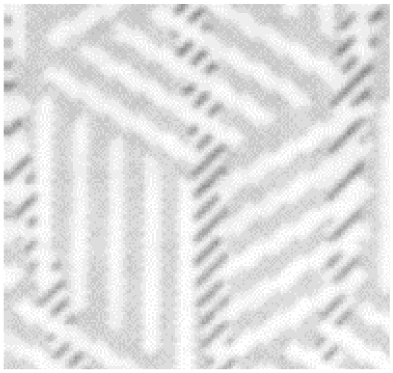
The "Holy Grail" of image-survivable security technology is a feature or features that could be authenticated using images already captured as the "normal" part of the sorting process. Such a solution would require no additional expenses or modifications to the different hardware platforms already in place. Unfortunately, this *appears* to be an unattainable goal.

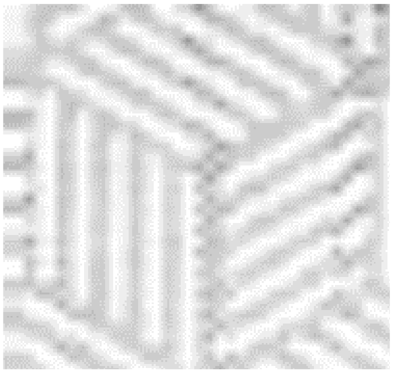
Most reader/sorters already capture images in two forms: a binary (black or white) .TIFF image and a 256 grayscale .JPG. Both images are captured at the resolution of the imager, which can be as high as 240 dpi on the IBM or as low as 100 dpi. The majority of existing imagers operate between 150 – 240 dpi. The binary image is usually available immediately upon capture for simple testing (but brief, as approx 25 items a second are imaged and processed) but the grayscale images can be reviewed in slower "off-line" processes after the item has been sorted.

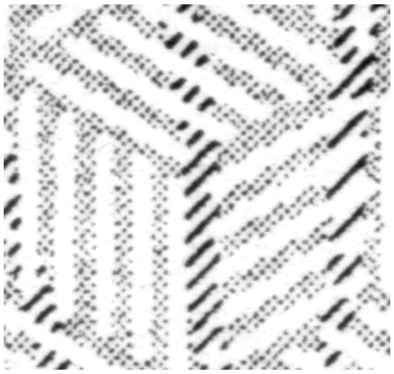
It is an understood rule that the resolution of copying equipment needs to be two times that of the original item to create an accurate reproduction. Since existing readers can only "see" at resolutions approaching 240 dpi, they are inherently unable to distinguish between the appearance of an original item or a copy reproduced at 480 dpi or more. Most consumer grade printers and copiers today operate at 600 dpi or greater, while commercial grade machines run closer to 1200 dpi and up, creating a presumption that most copies will be of sufficient quality to be interpreted as original items.

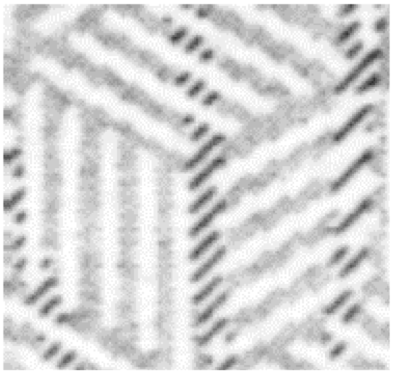
Consider these examples:

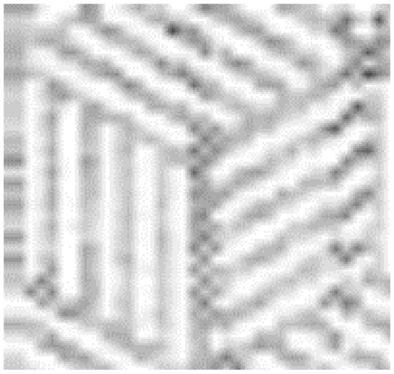

[1] Original Image


[2] 240 dpi grayscale


[3] 100 dpi grayscale


[4] B&W Copy


[5] 240 grayscale


[6] 100 grayscale

In this image set, we compare an original item at the different read/sort resolutions against a black and white copy. The samples demonstrate how accurately the copier mimics an original image, leaving the lower resolution scanners unable to distinguish differences in shapes between the original and the copy.

Interestingly, while the shapes of the dots are consistent between the original and copies, the grayscale conversion from color imagery does introduce variations in tone. Samples 5 and 6 are darker than samples 2 and 3 as a result of scanning the original blue versus the copy's black.

Unfortunately B&W copies are unlikely to be submitted in appreciable quantities as counterfeits to colored originals while color copies will mimic the original color and convert to a nearly identical lower resolution grayscale.

"Triggers"
Another obstacle to an effective image-survivable security device is the need to operate in an environment where most items will likely *not* include the feature. Personal checks are assumed to be completed by hand, and would benefit little from a security technology that identified original items, since personal checks are almost never copied or counterfeited but rather stolen and/or falsely issued. Since personal checks represent more than half all checks received for payment it would either be necessary for all personal checks to include the image-survivable security device or for the payment system to allow items without the device to successfully process.

In this either/or environment some kind of trigger becomes necessary to indicate to the reading system whether the security device is present. In a two-piece system like this, the entire security feature is only as robust as the *weakest* part of the system. I.e. disabling the trigger disables the security device regardless of how robust it is. This introduces an "infinite loop" problem: If a trigger needs to be present to search for the image-survivable security feature, the trigger itself must be both image-survivable and non-reproducible…

Even if a national standard were developed to define a common security process employable across all items, the standard would, by definition, become published and "open" to everyone needing to develop working products. Criminals would simply need to access the Net to learn exactly how to produce the necessary security.

Protecting Variable Data
Protecting against alterations requires one of two known approaches: comparing the information against a verification source like a database or encoded pattern, or flagging that the item has been tampered with. "Flagging" has been possible for years with the use of chemical stains but the advent of laser-printed originals has changed the landscape a bit as these items are easier to tamper with physically (with a pick or knife) than chemically. Toner anchorage technologies make it more difficult to alter original imagery but not impossible. Comparisons are available in two forms: on-document as in the case of encoded patterns or off-document as in the case of databases like Positive Pay.

Variable data can only be encoded when the variable data is available, requiring the use of special software and equipment to produce the items. This eliminates most consumer and small businesses that generate items by hand. And again, any encoding technique that became standardized would also likely become open to the public.

Positive Pay & Other Existing Solutions
Encoded barcodes and other proprietary solutions ultimately only work on final sorts where the decoding software/hardware is present and the systems already "know" the technology is expected on the items being processed. While these kinds of solutions are effective, at this point in the payment process we already have a simpler, and in some ways more robust, solution already in place in the form of Positive Pay.

Positive Pay, and its variations, employ a data file detailing all items issued against those received by the paying bank. If the item is not in the issued list, it is presumed to be fraudulent and not paid. Positive Pay is very effective for organizations that issue and/or print checks through computer systems since the same software that generates the items can be used to create the date file for the bank.

Positive Pay currently suffers from a couple of key shortcomings. First, while it protects the issuers and paying banks, it offers no protection to the bank of first deposit or those accepting the item. Second, in its primary form, Positive Pay utilizes the information easily processed by the reader/sorter: bank (R&T) account number, check number and amount. It is no coincidence that this is the MICR encoded content present on the bottom of the item. Criminals quickly recognized that the payee information not present in the MICR line remained vulnerable to fraud. Some emerging versions of Positive Pay attempt to use Optical Character Recognition (OCR) software to decode the payee information on the submitted item and compare against that provided by the issuer. However these are vulnerable to the limitations of the OCR software.

Point of Acceptance

The key to a successful item protection process appears to remain where it has always been: at the point of entry. Any fraudulent item that enters into the payment system ultimately costs somebody. While the banks are seeking to improve their ability to identify a fraud with an image-survivable security feature, thereby holding the fraud closer to the point of acceptance, the only solution that protects both the banks and their customers is one that makes it possible to recognize a fake when it is presented.

The fundamental failure of Positive Pay is its inability to detect fraud at the point of acceptance. Ultimately, a check is nothing more than an IOU provided by the issuer declaring that their financial institution will cover the amount entered on the note. Since Positive Pay ultimately “bumps” fraudulent items back to the point of acceptance it becomes the burden of the accepting institution to absorb the losses from bad checks. If an accepting institution or retailer cannot ascertain the legitimacy of an item with sufficient confidence, it is not bound to accept that item. Said another way, what good is your check if no one is willing to accept it for fear of fraud?

Clearly, at some point, it may become necessary for organizations issuing protected items to provide sufficient authentication techniques for acceptors of that item to ascertain their authenticity - not just to protect the issuing organization but to protect those who will accept their items. Providing these features doesn’t just minimize fraud throughout the payment system, it also preserves the reputation and legitimacy of the issuer’s negotiable instruments!

Positive Pay at the point of acceptance would help, but this solution has inherent problems. While the Internet could serve as a platform for a nationwide +Pay database to reconcile items, only those items uploaded into that database would function, leaving a large number of consumer and small business items outside the system. Another significant issue would be privacy. How does an accepting institution access this database without accessing all items issued by an organization? (Does every participating organization really want a detailed listing of who they write every check to, and for how much in a public database?). Finally, the acceptors themselves would have to address the added costs and processing times of executing the searches.

For the moment, the most successful protection technologies already in play appear to remain effective as we move forward with Check 21. Watermarks and Artificial Watermarks continue to thwart copiers. Thermochromic and Optically Variable Inks (OVI) continue to thwart counterfeits. Microprinting and High Resolution patterns continue to complicate fakes. Stains and coatings continue to complicate alterations. And all of these offer some ability for acceptors to identify attacks at the point of acceptance.

Image Based Solutions that Can Detect a Mimic

Having already illustrated the significant obstacles to developing an image-survivable security device that can function effectively at the existing resolutions of reader/sorters (above), the possibility still remains for an image recognizable solution. Those familiar with copy VOID pantograph technology understand that it is possible to craft printed patterns that grow or shrink when viewed and/or reproduced by conventional technologies. It is believed that through the use of a series of specially designed patterns that either grow or shrink depending upon the resolution of various reproduction equipment, it may be possible with sophisticated image processing software to differentiate between originals and mimics (ref Standard Register patents US 6.209.923 B1 and US 6.394.358).

Obstacles to overcome in such a solution include many of the problems already listed above: differentiating between items with and without the security device; establishing a standard while protecting the content of that standard; functioning within the multitude of colors and patterns employed on commercial checks; and even differentiating between a mimic and "natural" variations in production originals over the length of a run, and between multiple production runs.

In the end, regardless of the security solutions employed any detection software would be required to quickly sort through millions of low-resolution images, (each with known variations like color, background patterns, logos, payee, amounts, etc…), identify items that *want* to be authenticated optically, and accurately differentiate between originals and fakes. It is not clear to Standard Register at this time how such a software application could/would be developed but we do not dismiss the possibility of its development.

Legal Issues and Unintended Consequences

What is not clear in the above examples is the legal impact of this type of processing at the point of acceptance. It is understood by accepting institutions that under the current limitations of the payment system, checks rejected by paying banks are, for the most part, the liability of the acceptor. As scanning and reliable authentication are moved closer to the point of acceptance, the question of liability is likely to shift.

Check 21 does not require a bank to convert and truncate paper checks. It is voluntary.
A bank that chooses to convert paper checks into electronic images and substitute checks provides two warranties and an indemnity that travel with the substitute check. The two warranties are 1) that the substitute check is properly prepared, and 2) that no bank will be asked to make payment on a check that has already paid (no double debit).[2]

The indemnity is very powerful, and may well serve as a deterrent to banks eager to convert high dollar checks. It says 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."

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."

While Check 21 significantly speeds the handling and collection of checks, it is likely to stimulate significant growth in check fraud that is un-prosecutable. By introducing a conversion process that truncates, effectively destroying all evidence connecting a thief to an item, there is even less risk of arrest and prosecution to forgers than exists today. The Federal Reserve makes clear that there is risk to a bank that chooses to convert paper checks into electronic images and substitute checks.

From a defensive posture under Check 21, companies and individuals would be well served to use checks with excellent safety features that are not image survivable. These include true watermarks in the paper, thermochromatic ink, and paper or ink that is reactive to 15+ chemicals. These features would help authenticate the document visually, deter fraud attempts, aid in the detection of fraud at the point of acceptance, and potentially shift the liability for losses to the converting bank.

[2] Visit http://www.federalreserve.gov/BoardDocs/Press/bcreg/2003/20031222/attachment.pdf for the proposed rules governing Check 21 issued December 22, 2003. Read Page 74-75, Substitute Check Warranties.