

BITS

FINANCIAL SERVICES
R O U N D T A B L E

STRATEGIES FOR MITIGATING FRAUD RISKS ASSOCIATED WITH THE CHECK CLEARING IN THE 21ST CENTURY ACT

Background

The US payments system relies on physically transporting paper from one location to another, usually through intermediate points. The delay inherent in this process affects all parties to varying degrees. The maker may enjoy the float time from when he or she issues the check until it is paid. The payee may be required to wait until the check clears before gaining value. The depository institution must wait days to learn if the check is properly payable. And the paying institution must decide whether to pay items that holders in due course may later challenge. The essential weakness of this model was brought into stark relief during the week-long suspension of air travel following the 9/11 terror attacks.

The emergence of the Automated Clearing House (ACH), beginning with federal benefit payments to Social Security annuitants, represented the first systematic attempt to wean the payments system from paper. ACH and electronic funds transfer (EFT) network initiatives to introduce non-recurring paperless debits and the ubiquity of signature and PIN-based debit card transactions have contributed to a decline in paper check transactions. Still, more than 40 billion checks written each year remain a significant opportunity for alternative payments solutions.

Since electronic exchange of data and then imaging were first applied to payments, participants have sought ways to wring float out of the system by finding ways to “kill” paper as soon as possible. The efficiencies promised by electronic check presentment (ECP) have slowed because of the necessity of forming bilateral agreements between participants. And, while many banks post from ECP files, presentment for final payment remains tied to the physical receipt of the check.

The passage of the Check Clearing for the 21st Century Act (Check 21) in October 2003 marked a significant breakthrough—the point at which law finally overtook technology. Payments system participants are now scrambling to put technology and business practices in place to accommodate the anticipated October 2004 flow of image files and substitute checks.

In 1998, BITS established the Fraud Reduction Steering Committee to address the risks involved in the evolution of the payments system. The Steering Committee’s Electronification Working Group was formed in December 1999 in response to a series of initiatives designed to convert checks to electronic debits, primarily ACH debits. The Working Group’s first product was a white paper published in June 2000, *Electronification of the Paper Check in the U.S. Payments System: A Retail Banker’s Fraud Risk Perspective*. In September 2002 the Steering Committee sponsored a banker/vendor conference to seek technological solutions to risk issues arising from the then pending Check

Truncation Act. *The Evolution of Fraud Technologies in a Truncation Environment* was published after the conference.

This paper was written in response to a request from the BITS Executive Committee to assess the risk implications of Check 21.

Risks and Mitigation Strategies

Check 21 requires significant processing changes in the banking industry and presents new challenges in fraud detection and prevention. While the types of fraud will not necessarily change, we can expect that fraudsters will exploit those institutions perceived to be unprepared for the new environment. However, for those institutions leveraging new technologies based on digital imaging of checks, better fraud tools and reduced risk are possible. Most existing fraud detection tools will continue to be effective in a Check 21 environment. However, new image-based tools, combined with an acceleration of forward presentment and returns, will reduce check fraud in the long term.

Fraud risks and mitigation strategies are listed directly below.¹ The matrix at the end of this document describes Check 21-related risks and mitigants from the standpoint of the three major parties affected by the Act: the business customer that truncates checks before deposit, the bank of first deposit, and the paying bank. In the narrative below and matrix that follows, vendors and specific products are named. Neither BITS nor its members endorse any vendors or vendor products. References to specific products are for explanatory purposes only.

Risk: Counterfeit – The original check will not be available to the fraud analyst; instead the analyst will have to work from an image or substitute check. He or she will not have check stock color or paper stock to compare to other good items. Law enforcement will not have key pieces of evidence, such as fingerprints.

Mitigation Strategies

- Existing fraud detection tools, such as products that detect anomalous behavior, e.g., Carreker and Searchspace, Positive Pay, Teller Positive Pay, Payee Positive Pay and other vendor and proprietary tools, will continue to be very effective. Examining existing physical check security features will continue to have value when negotiating the check at the teller line.
- New image-based fraud detection tools that match check stock patterns and are able to detect differences in the expected check stock for each account will enable banks to review more checks at lower thresholds. For example, pre-authorized drafts (PADs) are becoming an increasing problem, but with image-based check stock pattern recognition, they can be easily recognized and reviewed via an image. Given the large volume of checks presented on a daily basis, this process is not possible in today's manual paper-based review environment.
- Image-survivable security features, if added to the check stock (consumer checks)—or even more effectively, added at the time of check issuance (large corporate accounts)—provide a security feature that can be interrogated from the image or IRD and matched to the check data on the image.²
- New image-based signature verification tools, such as FraudOne™, provide an opportunity to systematically review more signatures at a lower dollar threshold than is feasible with the current, manual signature review process. These tools greatly reduce today's high false-positive rates for counterfeit and forgery.

¹ Fraud categories are drawn from the American Bankers Association's biennial Deposit Account Fraud Survey.

² For example, 2-D bar coding, and seal encoding for corporate accounts.

Risk: Forgery – Because the original check will not be available to the fraud analyst, he or she will have to work from an image or substitute check.

Mitigation Strategies

- An image archive contains far better signature samples than most signature cards. Today, many banks still rely on outdated signature cards. Access to the archive provides many examples of more recent signatures that have been posted and are presumed good.
- New image-based signature verification tools, such as FraudOne™, provide an opportunity to systematically review more signatures at a lower dollar threshold than is feasible with the current, manual signature review process. These tools greatly reduce today's high false-positive rates for counterfeit and forgery.

Risk: Alteration – Because the original check will not be available to the fraud analyst, the analyst will have to work from an image or substitute check.

Mitigation Strategies

- Positive Pay remains the most effective tool for detecting dollar amount alteration. Image-enabled banks are able to offer their corporate customers enhanced Positive Pay with payee name verification, which detects payee alteration. However, until banks are able to deploy enhanced Positive Pay at the teller line, alteration will remain a significant risk.
- Image-survivable security features, if added to the check stock (consumer checks)—or even more effectively, added at the time of check issuance (large corporate accounts)—provide a security feature that can be interrogated from the image or IRD and matched to the check data on the image to detect alteration of the payee name or amount.

Risk: Kiting – Uncollected funds are moved among accounts in the same bank and to accounts at other banks.

Mitigation Strategy

- As image exchange adoption and presentment of substitute documents increase, the current two- to three-day float will be eliminated from the clearing process, making kiting more difficult.

Risk: Counterfeit Substitute Documents – Fraud operators could create counterfeit IRDs and present them for deposit or encashment.

Mitigation Strategy

- Presumably, the substitute check in the hands of a customer or non-customer would have been produced because the original check was returned for NSF or possibly refer to maker. However, it is more likely that a fraud operator would continue to counterfeit normal checks that would receive less scrutiny and pass more easily through the payments system. (While we do not view this as a significant risk, strategies are listed in the matrix at the end of this document.)

Risk: Expedited Rerecredit – Customers could file fraudulent expedited claims, counting on the reconvert bank not being able to provide an original check.

Mitigation Strategy

- Banks should maintain a claims database to detect customers making multiple claims, so that accounts can be closed if the claims are believed to be unfounded.

Risk: Destruction of the Original Check – Certain claims may require the original item. If the item is destroyed shortly after imaging, the item will not be available and may leave the reconvert bank liable.

Mitigation Strategy

- Banks should assess the relative risk and cost of storing transit items for a period of time and determine a method of retrieval.

Looking Ahead

Check 21 clearly changes the fraud risk profile, though not in a uniformly negative way. While new threats will arise because of the absence of the original paper check, their impact may well be significantly mitigated by the effective and efficient application of fraud filters and business practices already in use. Further, kiting and returned deposited item fraud will be harder to perpetrate because of the reduction in float.

About BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to www.bitsinfo.org.

Acknowledgements

BITS would like to acknowledge the following individuals who helped draft this paper.

Facilitator: Bob Jones,

RW Jones Associates, LLC

Richard Clausen, Bank of America Corp.

Chris Vaca, City National Bank

Lynette Brennan, Comerica Incorporated

Tom Slimick, Compass Bancshares, Inc.

Stan Sienkiewicz, Federal Reserve Bank of Philadelphia

Gary Swasey, Federal Reserve Bank of Philadelphia

Mike Thibodeaux, JPMorgan Chase & Co.

Sonja Kennedy, NetBank

Anne-Marie Blondin, The Bank of New York Company, Inc.

Frank Quaranta, The Bank of New York Company, Inc.

Catharine Gillespie, The PNC Financial Services Group, Inc.

BITS

1001 PENNSYLVANIA AVENUE, NW

SUITE 500 SOUTH

WASHINGTON, DC 20004

WWW.BITSINFO.ORG

(202) 289-4322

Check 21 Risks and Mitigation Strategies

PARTY AT RISK	FRAUD CATEGORY	SCENARIO	DEPARTMENT	MITIGATION STRATEGY
Bank of First Deposit	Forged Endorsement	Check is stolen and the endorsement is forged	Teller line	Manual verification to ensure proper endorsement
			Back office	Signature verification at set threshold, which could vary depending on size of institution, region, etc. Deposit fraud software , such as Carreker and Searchspace, helps determine if a deposit makes sense based on dollar amount, velocity, etc.
	Counterfeit	Attempt to deposit a fraudulent substitute check at an ATM	Back office	Sorter software to read position 44 of the MICR line to determine if a substitute check. Enact extended hold policy.
			Teller line	Paper/image comparison Velocity system software MICR readers Deposit fraud software (see above) Positive Pay Payee Positive Pay Image-survivable security features (such as 2D barcode, seal, etc.)
			Back office	Image comparison MICR readers Signature verification (see above) Deposit fraud software (see above) Positive Pay Payee Positive Pay Image-survivable security features (such as 2D barcode, seal, etc.)
	Attempt to deposit a fraudulent substitute check		Teller line	Take for collection. Enact extended hold policy. Refuse to negotiate.
			Back office	Enact extended hold policy.

		over the counter		
	Alteration	Check stolen from outgoing mail and chemically washed	Teller line	Positive Pay Positive Payee Image-survivable security features (such as 2D barcode, seal, etc.)
			Back office	Positive Pay Positive Payee Image-survivable security features (such as 2D barcode, seal, deposit fraud software, etc.)
	Insufficient Image Quality	Image is bad due to equipment issues, use of pastel gel pens, etc.	Point of transaction	Multilateral or bilateral agreements such as clearing house rules, regulations or operating circulars, with banks and others for which images are accepted, are strongly recommended to allow the warranties in Check 21 to flow back to the problem source. Image quality detection software.
Business Customer (Retailer, Check Cashier, etc.)	Forged Maker Signature	Checkbook stolen and checks used to purchase merchandise	Point of transaction	Signature/document verification (see above) Paper/image comparison MICR readers Velocity system software Image-survivable security features (such as 2D barcode, seal, etc.) Positive/negative databases (Scan, Telecheck, etc.) Refuse to negotiate.
	Counterfeit	Business check cashed	Point of transaction	Signature/document verification (see above) Paper/image comparison MICR readers Velocity system software Image-survivable security features (such as 2D barcode, seal, etc.) Positive/negative databases (Scan, Telecheck, etc.) Refuse to negotiate.
	Counterfeit	Attempt to deposit a fraudulent substitute check over the counter	Point of transaction	Signature/document verification (see above) Paper/image comparison MICR readers Velocity system software Image-survivable security

				features (such as 2D barcode, seal, etc.) Positive/negative databases (such as Scan, Telecheck, etc.) Refuse to negotiate.
	Alteration	Check stolen from outgoing mail and chemically washed	Point of transaction	Signature/document verification (see above) Paper/image comparison MICR readers Velocity system software Image-survivable security features (such as 2-D barcode, seal, etc.) Positive/negative databases (Scan, Telecheck, etc.) Refuse to negotiate.
	Insufficient Image Quality	Image is bad due to equipment issues, use of pastel gel pens, etc.	Point of transaction	Multilateral or bilateral agreements such as clearing house rules, regulations or operating circulars, with banks and others for which images are accepted, are strongly recommended to allow the warranties in Check 21 to flow back to the problem source. Image quality detection software
Paying Bank	Forged Maker Signature	Checkbook stolen and checks deposited or cashed at the teller line	Teller line	Manual verification (see above) On-us fraud software (such as Carreker and Searchspace) Deposit fraud software (such as Carreker and Searchspace) Positive Pay
			Back office	Signature verification (see above) On-us fraud software (such as Carreker and Searchspace) Positive Pay
	Counterfeit	Attempt to deposit a fraudulent substitute check over the counter	Teller line	Take for collection. Enact extended hold policy. Refuse to negotiate.
			Back office	Enact extended hold policy.
	Alteration	Check stolen from outgoing mail and chemically washed	Teller line	Positive Pay Payee Positive Pay Image-survivable security feature (such as 2D barcode, seal, etc.)

			Back office	Positive Pay Payee Positive Pay Image-survivable security feature (such as 2D barcode, seal, etc.)
	Duplicate Debits	Deposit of substitute check and secondary deposit of the original item		Software that recognizes posting of duplicate debits
	Insufficient Image Quality	Image is bad due to equipment issues, use of pastel gel pens, etc.		Multilateral or bilateral agreements such as clearing house rules, regulations or operating circulars, with banks and others for which images are accepted, are strongly recommended to allow the warranties in Check 21 to flow back to the problem source. Image quality detection software
	Expedited Recredit	Customer files fraudulent claim counting on the reconverting bank's inability to provide the original check	Back office	Maintain an internal claims database and/or subscribe to an industry database, such as the PPS Anti-Fraud Exchange, to detect customers making multiple claims so that accounts can be closed if claims are believed to be unfounded.