PARASCRIPT®

Check and Signature Fraud Prevention

Challenges and Resolutions

Takeaways

- *Checks remain a primary means of payment and are therefore the target of fraud.*
- *Check fraud results in huge losses increasing the need to pursue improved check fraud detection methods, including signature verification, check stock verification, courtesy amount/ legal amount (CAR/LAR) mismatch detection, and payee match positive pay.*
- *With AI and data, a Fraud Investigator can catch more fraud, review more items and increase workflow productivity – all leading to less exposure; the details are discussed in this paper.*

Summary

Checks remain the primary the means of fulfilling financial obligations. Technological advances coupled with increased availability at decreased costs have enabled criminals to engage in illegal and/or deceptive practices that include signature forgery, counterfeit checks and physical alteration of paper checks. Organizations can now benefit from a variety of efficient fraud prevention solutions that are cost effective for both large banks and smaller organizations.

What's in this paper?

Introduction

Payments are a fundamental part of the everyday life of our consumer culture and global economy. Payments are the engine that drives all forms of economic activity, affecting all businesses, organizations and consumers. Today we can choose from multiple payment options for any transaction: cash, checks, plastic cards, automated credit transfers, direct debits, online banking, mobile payments, etc. Regardless of payment method, consumers expect it to be secure and reliable.

Financial institutions and other payment processors must be service- oriented and committed to providing a variety of modern, user-friendly, efficient, and convenient payment options to customers in a time when exposure to payment fraud is greater than ever before. Payment fraud affects existing and emerging types of payment and has become one of the greatest challenges facing virtually all businesses and financial institutions.

The 2019 ABA Deposit Account Fraud Survey estimates check-related losses at $1.3 billion with banks preventing "91%—of attempted check fraud."[1] There are numerous ways these losses can occur as a result of forgery, counterfeiting, alterations, kiting, and embezzlement. Every time a new innovation is applied to an existing method of payment, or a new payment option is introduced, it leads to new methods and schemes by criminals to perpetrate fraud.

The situation may look like a vicious circle, but through analysis of breaches in each payment mechanism, a comprehensive approach to fraud control measures, and awareness and use of the most current technological defenses against fraud, payment system participants may significantly reduce risk and help avoid financial losses. An example of an innovation that offers an all-around defense to one of the most vulnerable payment methods – checks – is a check recognition solution comprised of image analysis and pattern recognition technology.

Check Payment Fraud

The payments landscape is changing due to the steady decline in check volume, the increasing use of the Automated Clearing House (ACH), and the continued growth of card, online and mobile payments. After many decades of providing the most efficient form of payment, check payment volume is decreasing, but organizations find it difficult to give up established and proven methods of payments perceived as secure and convenient.

Despite all the changes, consumers and businesses continue to use checks for a substantial portion of their payments. Checks remain the most widely used payment method and will keep this position for many years to come.

As a result, mass usage of checks makes them one of the most frequent subjects of fraud. Check fraud results in the loss of billions of dollars a year for banks, financial institutions and retailers, regardless of their size or location. It takes various forms of illegal and/or deceptive practices that includes signature forgery, counterfeit checks and physical alteration of the paper check. Identity falsification that had previously been the specialty of professional forgers has become widespread. Advances in technology are partly to blame. Highly-sophisticated, but inexpensive technology is now available to criminals, allowing them to access basic personal or corporate account information and produce hundreds of authentic-looking counterfeits or forged checks in a matter of hours.

Image exchange added complexity to the situation, because banks can no longer rely on the physical clues of paper checks such as color, smell and feel used in the past to identify fraud.

Highly-sophisticated, but inexpensive technology is now available to criminals, allowing them to produce hundreds of authentic-looking counterfeits in a matter of hours.

The image exchange paradigm shift and high level of perpetrator sophistication requires an increased level of analysis for institutions looking to protect themselves from check fraud losses. While criminals have access to more sophisticated technology with which to attack the weak defenses of companies, new technology is constantly evolving to arm financial institutions with multiple effective means to fight fraud. Today, there are a variety of efficient fraud prevention solutions that are cost effective for both large banks and smaller organizations. Moreover, check images allow the automation of many fraud detection processes that could not be done manually in the required volumes or accuracy levels.

Signature Forgery on Checks

Manual signature verification has been one of the most common fraud prevention methods during check item review process and has remained unchanged for many decades. During this time, signature forgery has become a serious security problem challenging financial institutions. According to industry studies, banks prevented $13.8 billion of check fraud, which totaled $15.1 billion in 2018.[1]

Clearly, with 14.5 billion checks written each year in the U.S.,[2] it is neither practical nor cost-effective to visually compare signatures on the number of checks processed daily. Nor has visual comparison proven to be reliable. Many banks have found that due to the increased volume of lower dollar checks and higher quality forgeries, many pass through a visual review undetected. Consequently, as the need to guarantee the authenticity of each document remains urgent, this task requires more efficient, controlled and reliable methods of signature verification.

Until recently, proposed technology for automated off-line signature verification did not offer an industrially mature solution, which was at least on par with visual verification. Today, state-of-the-art automated signature verification is a technology that can be easily adapted and efficiently applied to a financial institution's needs to detect and prevent fraud, regardless of the organization's type and size.

The most advanced systems reveal all types of signature fraud, including random and skilled forgery with accuracy rates that far surpasses visual verification. Such systems can contribute significantly to solving many check fraud-related business challenges faced by banks and other financial institutions. Benefits of automated signature verification include:

- The ability to process the images of checks, along with image replacement documents (IRDs), quickly and efficiently to identify suspicious signatures on a broader stream of images. These solutions allow financial institutions to lower the amount threshold for verified checks or inspect all checks instead of looking just at high-dollar items.
- The ability to reduce the number of false positive answers, i.e. the system accepting fraudulent signatures as genuine.
- Adaptability to existing environments and the ability to integrate with other fraud detection systems to create a centralized application that serves unique business needs.

- The opportunity to further improve customer service and satisfaction, enabling financial institutions to proactively inform customers, not only about potential fraud, but also about missing signatures, dates or other important information.

Automated Signature Verification: How It Works

Automated signature verification systems leverage the most state-of-the art artificial intelligence technology and the most comprehensive and advanced methods. In such systems, automatic comparison is executed by a powerful combination of verifiers using multiple, fundamentally different algorithms and techniques.

In particular, they combine a human-like holistic analysis of a signature and its segmentation with a subsequent analysis of the signature's elements using geometrical analysis, an analytical method based on signature segmentation and finding correlations between the fragments of reference and suspect signatures, dozens of neural networks and many other innovative techniques.

The whole verification process can be described as the work of a group of highly-skilled experts. Each of them has a favorite approach, which is especially efficient in specific cases and "good enough" in others. Additionally, each of them has a special area of expertise, which may be viewed as the distinctive characteristic of a particular verifier. When they are combined, their areas of expertise complement each other to result in excellent performance. Similarly, all signature verifiers apply various approaches to analyze dozens of a signature's characteristics.

Automated signature verification uses multiple reference images from any type of document to differentiate between characteristics of the signature and random deviations

Automated signature verification represents a bridge between the long-accepted practice of signing a document and the "reliable authentication and authorization" that is increasingly needed for financial institutions. It can provide enhanced security and control over the documents and transactions originated, transacted and stored in today's business environments.

Image-based signature verification in the back office can be efficiently augmented with a biometric signature verification solution at the point of presentment. The key to biometric verification of questionable signatures lies in reconstructing the writing motion and its elements.

Modern biometric signature verification systems benefit from combining multiple engines that analyze temporal biometric characteristics such as speed, acceleration, deceleration, stroke sequencing and length, pen pressure and timing information received directly during the act of signing, together with a proven innovative technology that scrutinizes signature shape. This allows biometric signature verification to be accurate, intuitive and fast, and making it ideal for front office applications.

Counterfeit Checks

Check stock verification software protects financial institutions against the fastest-growing source of fraudulent activity surrounding checks today: counterfeit checks. According to industry studies, "check fraud accounts for 47% of deposit account fraud losses."[1]

Counterfeit checks can be easily created either by duplicating a check with color copiers or by using a personal computer, scanner, bookkeeping software, and printer, which are all readily available today. Modern software allows those producing fraudulent checks to change some of the check's information, while keeping many valid check components.

Skilled counterfeits may even include the MICR line. As banks moved to the image-enabled check processing encouraged by the Check Clearing for the 21st Century Act, they are facing another challenge: many of the check's paper-based security features are lost, which makes counterfeit check fraud significantly more potent.

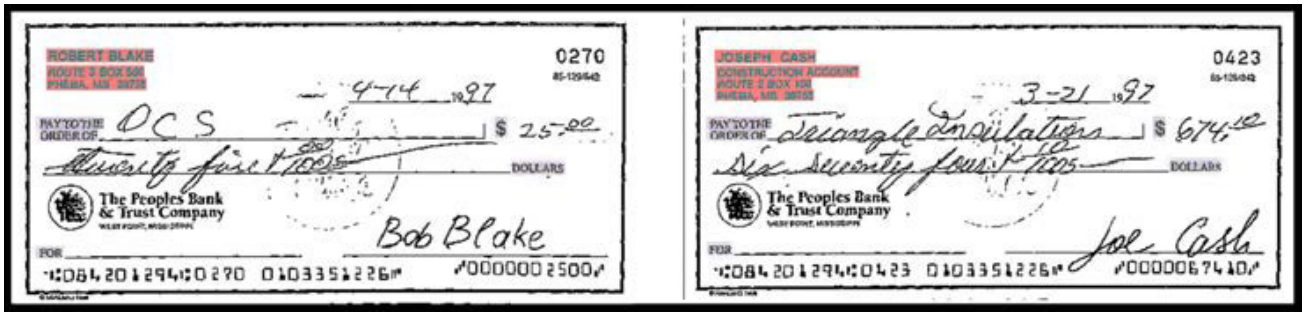
However, imaging offers many opportunities for improvements in check fraud detection and provides new powerful and efficient fraud detection tools as well. Image-based check stock verification software combats counterfeit checks by examining the check's format and features.

Automated Check Stock Verification: How It Works

Modern products for automated check stock verification are using secure filters for detecting the most sophisticated counterfeit checks and image replacement documents (IRDs). State-of-the-art systems developed using image analysis and pattern recognition technology are a secure and powerful filter for detecting even the best counterfeit checks. They provide scrupulous verification of all major preprinted elements on business and personal bank checks and IRDs offering the industry's highest accuracy and reliability.

The software goes far beyond merely examining each individual preprinted object on a check and comparing them against corresponding objects on a reference check stock. It scrupulously verifies the full image of a check as well as preprinted objects on a check including headers, such as: check number, date, payee, dollar amount, dollar sign, memo, payor block, and payor bank field. A combination of multiple forgery detection algorithms analyzes the elements' content, font type, font size, font spacing, the placement of each item and relative distances between pairs of blocks, allowing banks to immediately identify even the slightest variations on a given check. Multiple methods of verification – including quantitative analysis, pattern recognition, analytical and geometrical analysis and neural networks – ensure accuracy.

Advanced technology and methods allow check stock verification systems to work with equal efficiency on images scanned on different transports and reliably compare images, even if the input image presented for verification and the reference image have different resolutions. It also provides unfailing verification dealing with real-life documents having noise, stamps, marks, inscriptions, and other distortions. Due to the advanced optimization algorithms, even a minimally clean portion of an image is sufficient to ensure a reliable comparison.



The position of preprinted elements of checks is verified against reference checks

Automated check stock verification systems have been successfully implemented in many financial institutions and proved their robustness and capability for dealing with the challenges and requirements of real-life applications. They provide flexibility allowing elaborate decision-making schemes, the implementation of different scenarios of interpreting results, and efficient integration with alternative decision tools.

Check Content Alteration

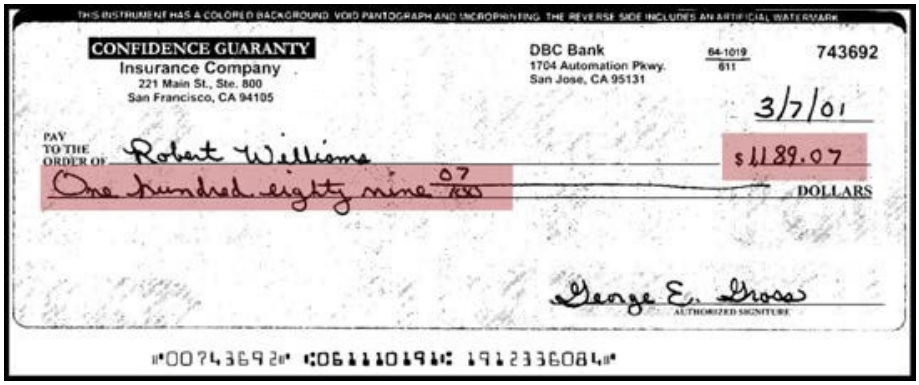
Alteration of check contents is another type of check fraud that challenges banks and financial institutions. There are different schemes and techniques that allow perpetrators to modify information on the original valid checks. Some schemes require special tools and sophistication, for example lifting bank officer approval stamps from one check and including it on another check of higher value or altering the MICR line with bogus information. Other alterations are easy: in many cases check writers leave spaces and gaps when populating the various fields; dollar amounts, payees and dates can be simply altered using a pen. Here is where image analysis and pattern recognition technology offers efficient solutions to uncover check fraud.

Courtesy Amount / Legal Amount Mismatch Detection: How It Works

The core capability of recognition technology is to recognize cursive handwriting, hand-print and machine print – individually or in any combination. For nearly a decade this technology has been used to read the numeric amount ("Courtesy Amount") and the text amount ("Legal Amount") fields on checks providing the most reliable solution for Proof of Deposit (POD) and remittance applications.

Proprietary, universal algorithms and state-of- the-art technology allow the location of the amount fields on any of check, regardless of the document's layout or style, and yield high accuracy and read rates even if extraneous elements such as noise, inscriptions, and teller receipt or cash register print data are present on the document. This technology also reads all kinds of other fields on checks and financial documents: payee name, check date, check number, MICR line, different alpha, alpha-numeric and numeric fields, etc.

The same proven image analysis and pattern recognition technology may also be used to detect Courtesy Amount (CAR) and Legal Amount (LAR) mismatch that usually results from a typical fraud scheme: amount alteration.



Courtesy and legal amount are automatically recognized and cross-validated to detect discrepancies

Sophisticated algorithms not only read numeric and text amounts and catch the potential discrepancy between them, but they also consider behavioral characteristics in writing checks and distinguish mismatches that may result from fraudulent activity from the typical check writer's errors and abbreviations. This helps to eliminate the number of false alarms and reduces unnecessary human intervention.

Payee Match Positive Pay: How It Works

Another efficient method of detecting alterations on corporate checks is positive pay. Positive pay is a bank service that proved to be one of the most effective anti-fraud tools available today for check disbursements. It allows the financial institution and its customer to work together to detect check fraud by identifying items presented for payment that the customer did not issue. The financial institution verifies checks received for payment against the list provided by the customer and pays only those on the list.

Any item presented for payment that does not match a corresponding item in a customer-issued file is flagged as an exception and the check is held for authorization from the customer that issued the check. Among the items detected by this process are forged checks having duplicate serial numbers, voided checks presented for payment, checks with altered or invalid amounts, stale checks, and checks with altered payee lines.

Positive pay services eliminate the need to review each check, helping companies gain control of the exceptions process and significantly reducing write-offs. Until recently, positive pay systems relied heavily on manual labor in reading the data from a check image and thus were very expensive to implement and manage.

Automating the identification of suspect items significantly reduces personnel costs related to research and reconciliation. It also raises the efficiency of the whole process. However, these systems did not recognize the payee name, which is a classical alteration on checks.

Automated payee match positive pay is an enhancement to the traditional image positive pay application. Image analysis and pattern recognition technology offers an automated solution for reading both machine printed and handwritten payee data from the check. This provides an extra layer of protection by comparing payee information from checks to the payee information provided in the customer-issued file, which was not accomplished or accomplished manually in the backroom operation of the financial institution.

The payee match positive pay application may be initiated immediately after the completion of the financial institution's In Clearing and Proof of Deposit check processing operation and traditional image positive pay process and allows financial institutions to further increase data validation on business checks and reduce check fraud.

Positive pay services eliminate the need to review each check, helping companies gain control of the exceptions process and significantly reduce write-offs.

Conclusion

Check 21 legislation and advancements in check imaging pose challenges, particularly in the fraud prevention and fraud detection area. Recognition technology presents effective means for financial institutions to maintain the highest level of account security. Another important benefit brought by Automated check recognition is that fraud filters can be applied not only at the back office, but at the front office. For example, positive pay can be integrated into the financial institution's branch system to detect fraud at the teller window or platform. When positive pay is extended from the back room to the branch, a check presented for cash at the branch mitigates fraud even further by using the payee information available to the teller at the branch.

The teller can compare not only the amount and check number, but also the payee on the check against the payee information in the issue file to make a pay/no-pay decision on the spot. Similarly, checks can be screened against electronic signature files and by check stock verification filter tools at the teller window, the retailer's point-of-sale, or the company's accounts receivable department.

There is an arsenal of reliable and cost-effective automated tools that can effectively prevent and detect check fraud. Financial institutions using these technologies show that the benefits are numerous and include timely fraud prevention, the mitigation of fraud losses, protection of the bank's assets and improved customer loyalty.

Sources

[1] *"ABA Report: Banks Prevented More Than $22B in Fraud Attempts in 2018."* ABA Banking Journal. *January 15, 2020*

[2] *The 2019 Federal Reserve Payments Study*

About Parascript

Parascript software — driven by data science and powered by machine learning — configures and optimizes itself to automate simple to complex document-oriented tasks such as document classification, document separation, and data entry for payments, lending and AP/AR processes. Every year, Parascript software processes over 100 billion documents in the banking, government and insurance sectors. Parascript offers its technology both as software products and as software-enabled services to our partners. Our BPO, service provider, OEM and Value-Added Reseller network partners leverage, integrate, and distribute Parascript software in the U.S. and across the world. Visit us at **www.parascript.com.**

Contact Us to get your demo or call us at **888.225.0169** to speak with an expert.

6273 Monarch Park Place, Longmont, CO 80503 USA
T: 888.225.0169 | F: 303.381.3101 | info@parascript.com

PARASCRIPT®

GET IN TOUCH

info@parascript.com

parascript.com

(888) 225-0169

6273 Monarch Park Place, Longmont, CO 80503 USA
T: 888.225.0169 | F: 303.381.3101 | info@parascript.com