



A Holistic Approach to Reducing Check Fraud and Identity Theft

- White Paper -

**SOFTPRO Group
May 16th, 2006**

© SOFTPRO – www.fraudone.com

SOFTPRO NORTH AMERICA, INC. 750 South Madison Street Suite # 310 · Wilmington · Delaware 19801
.....Tel: +1 302 504 0606 · Fax: +1 302 504 0604 · info@softpro-na.com.....

International Offices:

SOFTPRO GmbH · Wilhelmstrasse 34 · 71034 Boeblingen · Germany.....
.....Tel: +49 (0) 7031 66 06 - 0 · Fax: +49 (0) 7031 66 06 66 · info@softpro.de
SOFTPRO UK Ltd. 16 St Cross Road · Crondall · Farnham · Surrey GU10 5PQ · United Kingdom
.....Tel: +44 1252 850 180 · Fax: +44 1252 850 180 · softpro-uk@softpro.de
SOFTPRO SOFTWARE PROFESSIONAL ASIA PACIFIC PTE LTD · 25 Internat.l Business Park #02-12A · Singapore 609916
.....Tel + 65 562 9054 · Fax + 65 562 9055 · softpro-ap@softpro.de.....

A Holistic Approach to Reducing Check Fraud and Identity Theft



Abstract

Due to legislative changes, and the increasing sophistication of fraud criminals, the banking industry has an acute need for next-generation fraud solutions. In particular, check fraud and identity theft related losses are costing the banking industry billions of dollars every year. An architecture for effectively reducing check fraud losses while simultaneously reducing internal paper processing costs is presented. The architecture is based on both back, and front office components. The back office components provide a cost-effective way of identifying check fraud by combining multiple image processing and transaction based components within a single framework thus avoiding expensive and complex integration effort. The front office components take advantage of legislation that allows the capture of electronic signatures within documents such as account opening forms and other contracts for enabling paper-free processes while simultaneously providing the ability to uniquely identify customers based on a non-intrusive biometric signature.

A Holistic Approach to Reducing Check Fraud and Identity Theft



Increase in Fraud Perpetration

In the last two years, massive changes have taken place in the banking industry which have led to, or have facilitated a clear increase in fraud perpetration. The changes can be categorized into the following two general groups:

- Government legislation: Recent laws have opened new opportunities for fraudsters, but may also be used to diminish the risk of fraud.
- Increasing sophistication of fraudsters and increase in fraud attempts

Two legislative changes are particularly interesting to the banking industry with respect to fraud perpetration, as well as cost savings. The first is the Check 21 Act passed in 2004. The second is the E-Sign act passed in 2000.

Check 21 Act

The Check 21 Act requires financial institutions to accept electronic images as legal substitutes for paper checks. The law was originally conceived to enable the ability to continue financial transactions in the event of a catastrophe such as the 9/11 events. The primary goal of the legislation is to facilitate the widespread use image-based check transactions.

Image-based check transactions have many obvious advantages for financial institutions. The use of images as a paper substitute provides increased transaction robustness (e.g. less correction items, quick retrieval of items) and cost savings in terms of space management (archival space). However, with this approach checks are electronically truncated at the point of capture so that all subsequent processing is based on image exchange only. Electronic images do not have the advantage of paper-based security features such as feel, color or smell.

An image-based processing environment may or may not use truncated images. The Check 21 image replacement documents are truncated. Truncated images further complicate the use of traditional image-based fraud detection tools that assume a "full size" image such as pattern matching-based signature verification. Such tools must now work with different sizes of images and can no longer rely on pure pattern matching, but instead need to match signature and stock characteristics in an intelligent way.

For financial institutions, the move to support Check 21 takes time and careful planning not only because of the introduction of supporting technology, but also because of the necessary fraud prevention measures that must be taken. New opportunities abound for fraudsters because many institutions are inadequately prepared to deal with the disruptive effects of introducing image technology, and especially with the effects it can have on fraud susceptibility.

According to the ABA (American Banker's Association), check fraud accounted for more than \$5.5 billion in losses in the United States alone in 2004. This was up from the 2001 losses of \$4.3 billion. Organized crime rings have recognized this and have thus become more active in this type of crime. The crime rings exploit knowledge of bank detection methods and have the resources to maximize their gains. For example, a typical crime scenario is to send out a group of perpetrators under false identities to pass counterfeit checks with the goal of determining a bank's minimum amount threshold for verifying checks. This can only be done in a concerted effort with enough

A Holistic Approach to Reducing Check Fraud and Identity Theft



manpower. However, once the thresholds are determined, the bank is open to a number of undetected fraud possibilities.

Banks that have moved, or are in the process of moving to an image environment are in a weak position without an effective image-based fraud prevention system. To make matters worse, law enforcement agencies in most countries are not equipped to either investigate or prosecute the majority of fraud attempt cases. So, not only is the crime lucrative, but there is also a very low risk of being caught and being sentenced to jail.

The two main types of check fraud perpetrated, according to the American Banker's Association (ABA) Deposit Account Fraud Survey Report in 2003, are forged signature maker and counterfeit checks which together account for 39% of all check-related fraud in the United States (see figure 1 below). This number is growing consistently every year. Similarly in the UK, check fraud attempts increased by 20% between 2004 and 2005 to a total of £665 million in potential fraud losses. This indicates that the use of checks as a vehicle for fraudulent transactions is a global phenomena. This trend is likely to continue in the near future as more banks world wide introduce electronic processes.

Forged signatures are the most effective way of perpetrating fraud because crime rings are aware of the fact that it is unrealistic for a bank with large transaction volumes to verify every signature on their inclearing items. Generally, the verification involves a tedious manual process which is only used for larger transaction amounts.

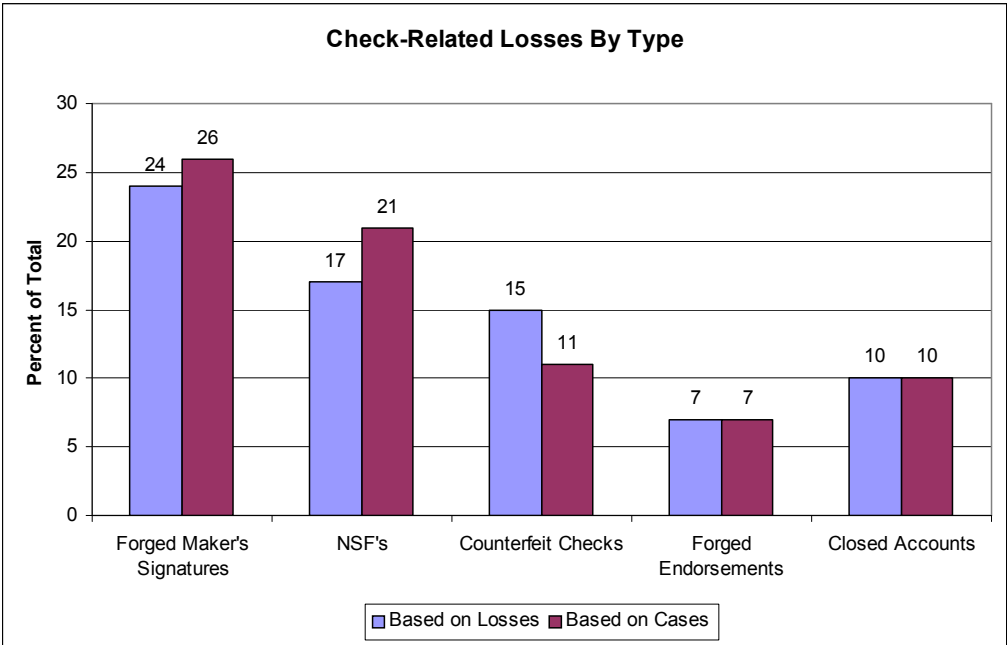


Figure 1: A Check-related losses in the United States¹.

¹ Source 2003 ABA Deposit Account Fraud Survey Report

A Holistic Approach to Reducing Check Fraud and Identity Theft



In the United States, counterfeit checks are most commonly created using a modified check stock i.e. check design. US banks permit the use of non-standardized check stock allowing two different customers of the same bank to have differing check designs. Similarly, a single customer may use several different check designs. A common example of this is a corporate customer who may have several different corporate designs. Although convenient for end-customers, non-standard check stock poses a challenge in terms of fraud susceptibility. Since valid checks on a given account may look completely different from each other, a fraudster can easily exploit this vulnerability to create an authentic looking counterfeit using their own check stock. In many cases, neither the bank nor the fraudster knows what the real valid check stock looks like. The challenge is to be able to distinguish between good check stock and counterfeited fraudulent check stock in an image-based environment. In other countries, counterfeit checks consist of other alterations, or complete copies of original, valid check stock.

For both forged signature maker and counterfeit checks, the fraud trend is towards targeting lower transaction amounts rather than smaller numbers of large transactions (see Figure 2). By reducing the check amounts, criminals are exploiting the fact that banks prioritize fraud investigation on checks over a certain limit. This increases the importance of being able to automatically verify images so that even lower amounts may be verified. Only with an automated process is it possible to prevent fraudulent transactions in large volume environments to pass through undetected.

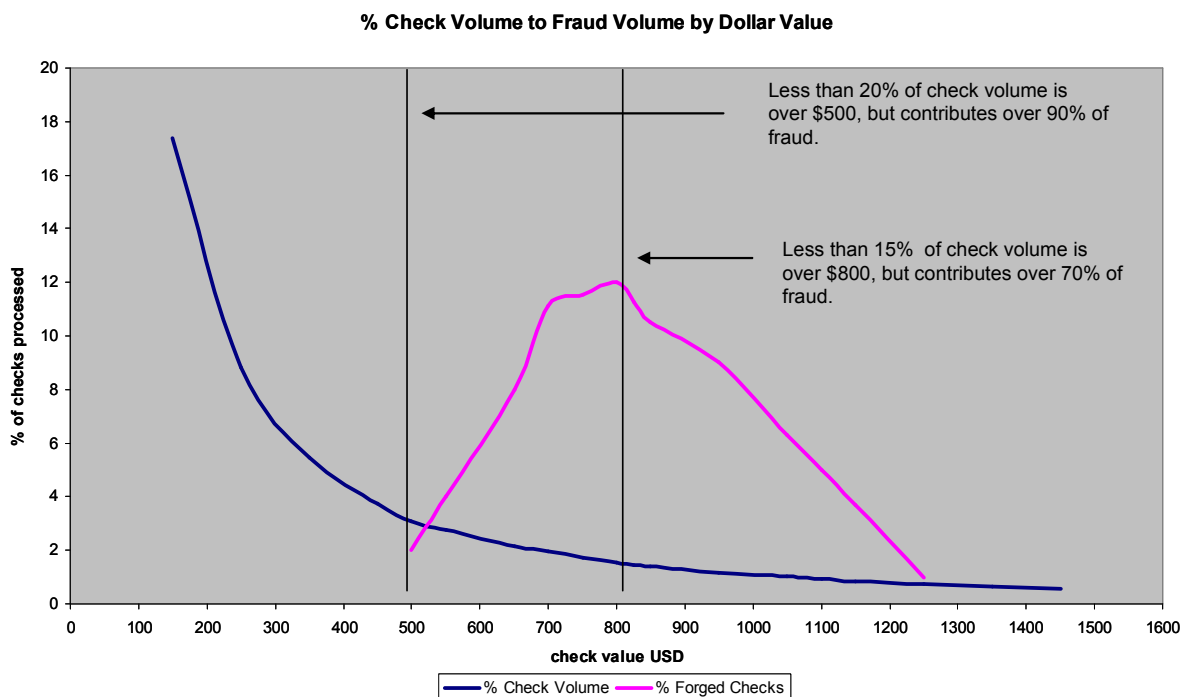


Figure 2: A Trend toward lower amount fraud transactions²

² Source: Banking Strategies, March/April 2003, p. 30

A Holistic Approach to Reducing Check Fraud and Identity Theft



E-Sign Act

Driven by expense reductions and other benefits related to replacing paper-based processes by electronic ones, governments all over the world have been passing legislation to pave the way for the acceptance of dynamic signatures as a legally binding form of authorisation and authentication. Most notably, the E-Sign Law (Electronic Signature in Global and National Commerce Act) passed by the US government in October 2000 has granted legal status to electronic signatures in the US by giving them the same legal weight as traditional ink signatures on paper. The E-Sign law presents an opportunity for banks to capture an electronic signature from their customer at the time of entering into any legal agreement (e.g. the opening of a new bank account). This not only presents huge cost savings related to the elimination of paper-based processes, but also the opportunity to capture a uniquely identifying characteristic of their new customer which can be used at a later point in time to prevent identity theft based fraud. There are several biometrics that can be captured, digitized, and used as an electronic signature such as a fingerprint, facial scan, or iris scan. However, the capturing of these biometrics for use as a digital signature often conveys a sense of criminality to the end-customer. This is particularly undesirable in situations where a bank would prefer to convey a sense of trust to their new customers, such as during the opening of a new account.

In the business world today, contracts are sealed using a handwritten signature. Handwritten signatures are the most culturally accepted form of authorization. Therefore, when moving from paper to electronic contracts, the ideal solution would be to capture a handwritten signature electronically to seal a contractual agreement. A handwritten signature can be used for signature law compliant electronic processes. However, this is only possible if the electronic representation of the handwritten signature contains more than just the image of a signer's signature. The signature must be unique to the signer, not forgeable, and be associated with the signed document in a way that the document cannot be modified after signing. Ideally, the electronic representation of the handwritten signature must contain information about the dynamic characteristics of *how* the signature was signed such as speed, patterns, habits, and pressure of pen strokes. Together, these characteristics represent a biometric footprint, *or dynamic signature*, which is unique to every individual and can not be reproduced by a forger even if the forger is aware of what the real signature they are forging looks like. Figure 3 depicts both the static and dynamic characteristics required to uniquely identify a signature. In addition to advantages such as the cultural acceptance of signatures, dynamic signatures also offer some of the best biometrics with respect to uniqueness and repeatability so that they can effectively be used to identify customers.

Capturing dynamic signatures has the following advantages for financial institutions:

- Cost savings due to legally-binding paperless contracts and associated processes
- Ability to identify customers in real time when they make transactions at branch offices but without conveying a sense of mistrust.
- High quality, "noise-free" signature references due to direct capture instead of traditional scanning process which leads to an improved forged signature maker fraud detection.

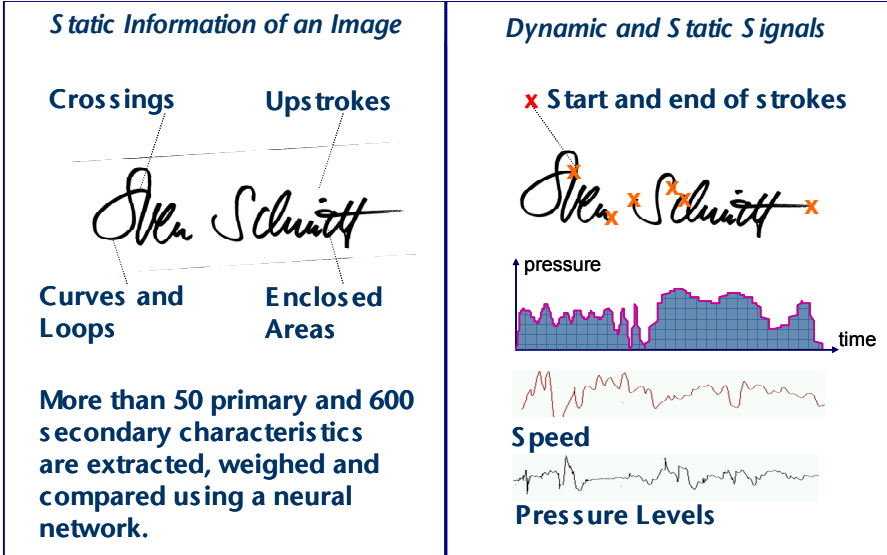


Figure 3: Static and dynamic characteristics of a handwritten signature

Fraud Detection Silos

Over the past five years, there have been a number of technology vendors that have marketed image-based check fraud detection solutions. These solutions focus primarily on a single technology such as signature verification, check stock verification, or 2D barcodes for detecting fraud i.e. technologies that zero-in on a single fraud characteristic type (e.g. forged signatures in the case of signature verification). A single-technology approach has its merits for finding fraud based on a single characteristic type. However, it also has two major disadvantages:

- It does not detect any fraud that uses another characteristic.
- If a fraudster knows that a bank has a system in place to detect this type of characteristic, they will manipulate a different one.

Often, it is a combination of characteristics that will identify a transaction as being fraudulent. Optimally, a financial institution would be able to use every technology available in every possible combination to identify a bad transaction. Additionally, it would be able to take into account external factors such as geographical regions (e.g. a particular state may see more fraud of a certain type than another).

Unfortunately, there are good reasons why these institutions don't simply buy every technology and build a federation of fraud detection technology. Fraud detection systems, as the name implies are based on a *system* of components that each center on a single fraud detection technology. If a customer wishes to use more than one technology, more than one system is required. Since these systems are almost always orthogonal, their implementation in the

A Holistic Approach to Reducing Check Fraud and Identity Theft



customer's internal infrastructure leads to extensive investments in order to:

- install, and maintain each individual system
- integrate each of the systems with existing back office processes
- supply check images to each system individually

More often than not, the investment outweighs the fraud loss reduction benefit. So, the key to a successful fraud detection implementation is to invest just enough so that the overall costs are lower than the loss being prevented. One measure of effectiveness for fraud detection systems is the proportion of *false positives* to the actual number of fraudulent items. That is, the number of items that a fraud analyst must look at before they find a real fraudulent item. The higher the number, the less effective the system is, and the more expensive the fraud detection process becomes. The typical homegrown solution consists of many silo systems each focusing on a particular aspect of fraud detection, and combined through complex communication and data interfaces to produce a superset of fraud suspects. This has several disadvantages:

- The implementation of the interfaces is a complex task requiring constant maintenance due to changing data specifications.
- The number of false positives increases dramatically as the number of fraud suspects increases.

The ideal solution must approach the problem of fraud detection differently in that it must not focus on one single technology, but rather supply a platform (*the system*) into which many different technologies may be plugged-in and combined as best-of-breed *engines*. Each engine concentrates on a single aspect of image-based fraud detection. The solution must complement rather than compete with already existing fraud detection systems by providing standardized interfaces for integrating information from external systems into the decision process. It must have the ability to easily combine, weight, and score results not only from the multiple individual technology engines, but also from the multiple external systems. This secures the investment already made into existing fraud detection systems. Lastly, decisioning technology must be incorporated into the solution to reduce the number of false positives, and more effectively recognize fraud patterns. The decisioning must be rule-based and easily configurable so that it may be quickly adapted as fraud patterns change.

The immediate benefits of such a solution are:

- Completely image-ready environment (also Check 21 ready)
- Unparalleled fraud detection due to a combination and consolidation of technologies
- No need to invest in several large incompatible systems
- Minimal integration effort
- Selection of relevant fraud technologies seamlessly applied to a bank's individual fraud environment
- Ability to quickly react to the ever-changing fraud environment

The two primary check fraud attempts are forged maker signature and counterfeit checks with an increase in fraud based on PADs (pre-authorized drafts). Additionally, these types of fraud are

A Holistic Approach to Reducing Check Fraud and Identity Theft



often perpetrated by criminals who have assumed a fake identity. Therefore, to effectively stop these types of fraud, the following verification engines should be key components in a detection strategy:

Back office fraud components:

- **Signature Verification:** matches signatures against known good references to assess whether or not a signature has been forged or not. This includes rule verification for accounts with complex signing rules (e.g. Joe may sign with Jim for a maximum of 2000\$ until May 15th)
- **Check stock Verification:** Compares a check image with known good references to detect discrepancies compared to the original check's stock. E.g. difference in address block size
- **Pre-Authorized Draft Fraud suspect detection:** Automatically detects whether or not an item is a PAD, and if so whether its payee is on a bank-specified black list.

Front office automation components:

- **Real-time dynamic signature verification:** compares the dynamic characteristics of a person's signature with a reference signature to determine if they match. The reference signature may be captured at the time of account opening, or any time thereafter.

The key technologies used should not be limited to the above fraud detection components, but must ideally include bank internal information such as customer information files, or input from an existing external system such as a transactional behavior analysis system. All relevant information that can be used in any way to identify a fraud pattern should be incorporated into the overall fraud detection strategy.

Fraud detection architecture (inclearing back office)

The figure below (see Figure 4) depicts the architecture that has been described above and how it fits into the overall item processing infrastructure of a bank for effectively detecting check fraud. The goal of the architecture is to provide a cost-effective solution for detecting check fraud that enables many different technologies within the same system rather than a loose integration of many complex systems.

The architecture consists of both client and server-based components. At the heart of the architecture is the verification infrastructure. The infrastructure allows the plugging-in of various fraud-detection engine technologies and provides the overall load-balancing for the processing of the daily inflow of checks to be cleared by the bank. As part of the infrastructure, components are provided for interfacing to the bank's back office systems for loading images of checks to be processed. In this way, the architecture can be easily incorporated into the existing inclearing infrastructure.

A Holistic Approach to Reducing Check Fraud and Identity Theft

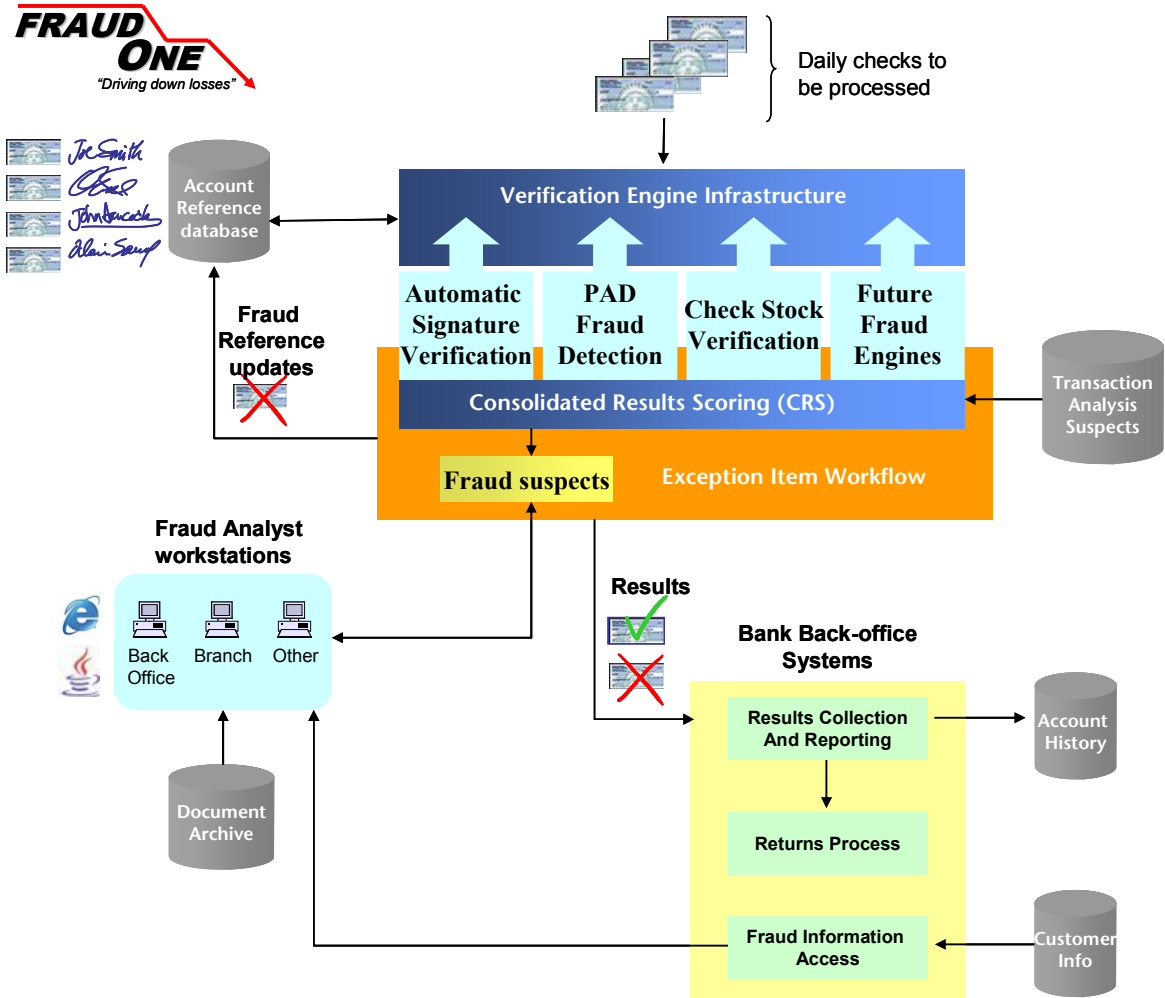


Figure 4: A plugin-based check fraud architecture with combined risk scoring

The daily check images may be Check-21 IRDs (Image-replacement document), or images of inclearing checks that have been scanned by the bank’s scanning facilities. During the verification process, the verification components need access to information regarding the accounts for which the checks are being cleared. They retrieve this information out of the account reference database. The type of data stored in this database depends on the verification engines that are plugged into the infrastructure and typically consists of signature (both static and dynamic) as well as check stock image data. As with the daily check items, interfaces are provided for loading the data into the account reference database. Additionally, the reference data may be accessed and modified by bank personnel via a web-based client application.

Once loaded, the check images are routed through an exception item workflow which is responsible for passing items to the various server components of the system for verification in a *chain-like* manner. It does this internally by putting the items into various processing *queues* each

A Holistic Approach to Reducing Check Fraud and Identity Theft



of which is served by a single component of the system. Once an item is processed, the system passes its results to the next component in the chain via the workflow. In this way it is possible to have images processed by multiple fraud detection engines.

The results of the different engines are then consolidated by the *Combined Risk Score (CRS)* component to determine whether or not they pose a fraud threat i.e. whether or not they are suspicious (see Figure 5). The CRS engine is an integral part of the item processing workflow and uses rules that are defined based on the bank's current fraud profile to weight and score results. The CRS engine not only uses results from the individual fraud detection engines, but also has standardized open interfaces to allow the incorporation of results from external bank systems such as transaction analysis systems or customer information files in the overall fraud scoring. By combining the results and allowing the bank to set different weighting to different fraud characteristics, a more accurate fraud detection can take place. In addition, the cost of fraud detection is minimized due to the significant reduction of false positives allowing analysts to concentrate on real suspects.

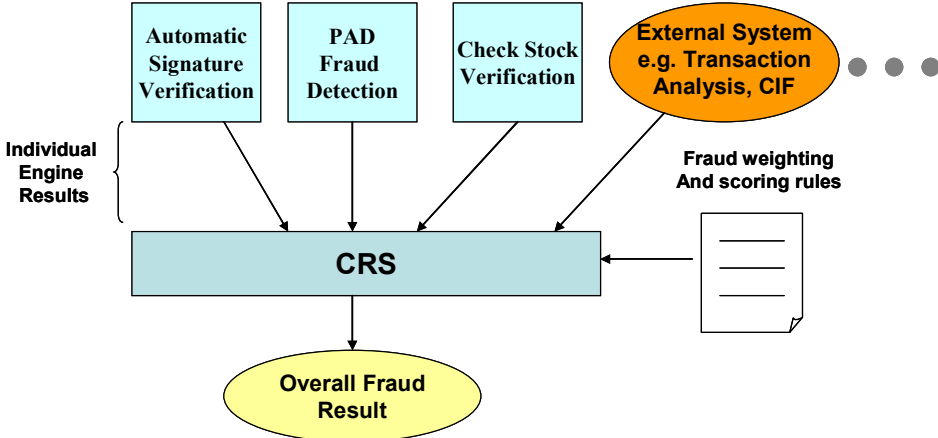


Figure 5: combined risk scoring to create a consolidated result

Based on the results of CRS processing, suspected items are placed into a visual verification queue for review by the bank's fraud analysts. Fraud analysts access the queue via the *fraud analyst workstations* which are client software applications that enable access to the back office system via a thin web browser, or a full locally-installed client application. Due to its distributed architecture, fraud analysts are able to view the suspected items from different parts of the organization (back office, or branch) so that the system can be configured to fit into the bank's infrastructure and not vice versa. These analysts usually have access to other internal fraud information via the bank's back office systems (e.g. account document archives). The analysts will typically use a combination of the results provided by the combined engine scores, and their own information to make a decision as to whether an item should be treated as real fraud. If this is the case, the result is sent back to the back office via the workflow where the final result is output from the system. The final results are then used by the bank's returns department to process the item as an exception.

A Holistic Approach to Reducing Check Fraud and Identity Theft



To ensure that the data is kept up to date, two types of information are sent back to the account reference database after processing:

- A list of new references (e.g. new signatures, or check stock)
- A list of fraudulent items, also called *fraud feedback*

During the fraud feedback process, reference data that is known to have had fraud attempts may be marked as such so that further transactions on the account can be treated with high suspicion, or even completely blocked.

Preventing Identity theft by “*knowing your customer*”

One of the key components in the fraud detection architecture described above is signature verification to detect forgeries. In order to be able to use such a system, reference signatures must be available in an *Account Reference database*³. There are several methods for creating a reference database. The simplest method is to scan reference signatures from archived signature cards. However, this method is often neither practical nor effective due to the large number of signatures that are actually on paper file, and the age of the signatures. Additionally, a person's signature slowly changes over time. This can sometimes cause older signatures on file to be poor references. Another method for creating the reference database is to extract the signature from an inclearing check, also known as “lifting”. With this method, images of signatures can be captured on the fly as checks on a new account are drawn for the first time. These signatures are also called “static signatures” because they represent the non-changing characteristics of a person's signature. The above architecture must provide the interfaces as part of the verification engine infrastructure to be able to do this effectively for an unlimited number of signatures⁴.

Although effective, lifting images from an inclearing check has two drawbacks:

1. The quality of the signature image may be poor (noisy, badly cropped) thus affecting future verification results
2. Only the “image” (i.e the static characteristics) of the signature can be captured thus it cannot be used to truly identify a live person later.

A third method of creating the reference database is to capture the signatures electronically at the time of account opening, or any other bank-customer relationship contract creation such as a mortgage application. In this method, an input device is used to capture both the static and dynamic characteristics of the customer's signatures at the same time. The signatures are embedded in the contract in a legally binding way according to respective legislation. The

³ The account reference database must also include reference images of approved check stock for a given account if check stock verification is to be used.

⁴ Both the scanning and „lifting“ method described here can be used to populate the reference database with check stock images as well.

A Holistic Approach to Reducing Check Fraud and Identity Theft



signatures are immediately registered in the reference database, and the associated contract is stored in a document archive (see Figure 6). This method has several advantages:

1. The signatures are immediately available for check verification. This avoids delays in the signature availability which are often exploited by fraudsters.
2. Since the signature represents a “biometric footprint” unique to the signer, the signature may be used by the same front-end system for confirming the identity of the signer at a later date thus eliminating identity theft and enabling the bank to “know its customers”.
3. The quality of the signatures captured this way are much higher than from a scanned image since they are noise-free thus significantly improving the quality of the static signature verification during the inclearing process.
4. Capturing signatures directly within the signed document enables a completely paperless contract process leading to both significant cost savings (printing, scanning, sorting, archiving, etc.) while improving the image of the bank with its customers

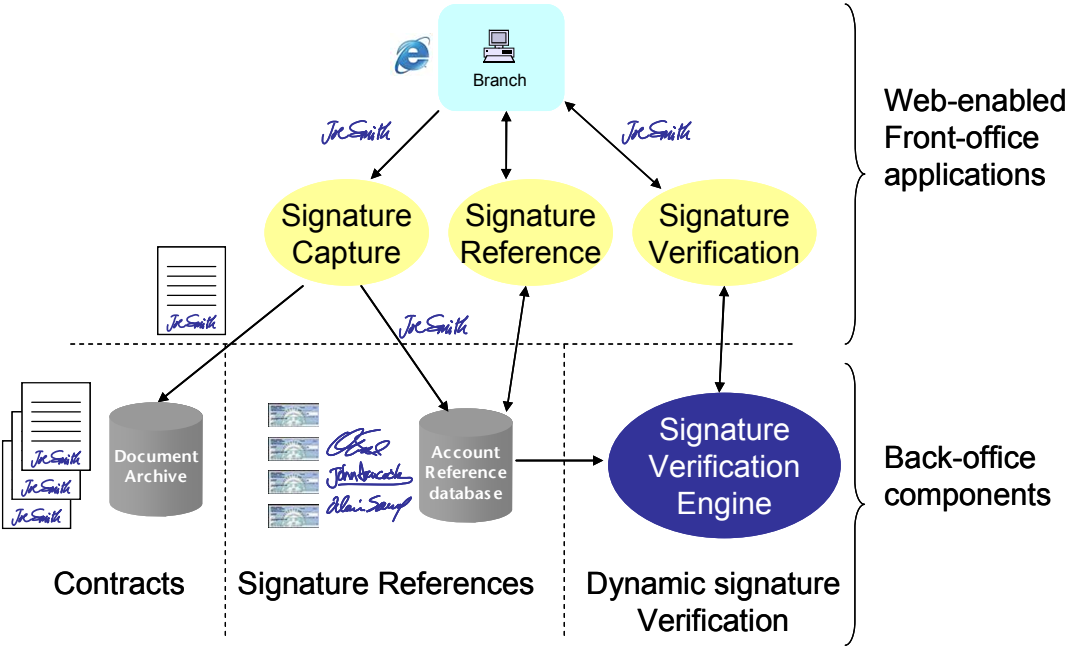


Figure 6: Capturing of dynamic signatures at the branch for later verification

Although capturing dynamic signatures is the optimal solution for building the reference database, it does have the drawback that the signer must be physically present to provide the reference signature (e.g. during the account opening ceremony). A complete database would thus require all customers of the bank to come in to their local branch and sign their name in person to be

A Holistic Approach to Reducing Check Fraud and Identity Theft



stored in the reference database. Obviously, this is not practical. However, if the system can support the verification of both static and dynamic verification, then a combined solution can be provided where the static image (captured via lifting) can be used for verification until the customer has either entered into a new contract with the bank, or has come into the branch to provide a dynamic signature. This enables the bank to immediately take advantage of the signature verification capabilities while progressively adding the dynamic signature capabilities over time.

Open Architecture as an application-enabler

The platform architecture described in this paper has been implemented⁵ and proven to be successful at effectively identifying fraud in large installations processing millions of checks per day. Just as the platform is flexible in terms of technologies, it is also flexible in terms of how it may be expanded to serve other applications. The combination of engine technologies combined with CRS risk scoring may be employed to create rules for identifying fraud that are not purely check related. For example, the system could be used to combat money laundering, or tracking transactions from particular individuals for security reasons.

Summary

The banking industry is facing a serious risk in the form of check fraud and identity theft related losses. In order to fight these threats in a cost-effective manner, an architecture must be employed which is designed to ensure that the cost of fighting fraud is less than the actual loss incurred. This is only possible by combining technologies in a single consolidated platform. At the same time, the architecture must be flexible enough to react to both short-term fraud trends, as well as long term trends that may require new processing technologies to be added as new threats arise. The most effective way of preventing fraud before it arrives at the back office in the form of a check or other transaction, is to “know your customer”. The accurate identification of a customer at a branch, can reduce identity theft related losses while. Using the added benefit of dynamic signatures to do so, a bank can reap immense cost savings by moving to paperless processes while improving its capability to identify fraud.

⁵ SOFTPRO's FraudOne[®] product already employs the concepts described in this paper

A Holistic Approach to Reducing Check Fraud and Identity Theft



About SOFTPRO

SOFTPRO is a worldwide leading provider of transaction security solutions with offices in the United States, Germany, United Kingdom, and Singapore. The company focuses primarily on check fraud detection, signer authentication to reduce identity theft, and enabling paperless processes such as bank account opening applications using biometric signature technology. SOFTPRO's automatic signature and check stock verification solutions have been successfully deployed at more than 250 banks worldwide.

About FraudOne®

FraudOne® is SOFTPRO's flagship product family focusing on fraud prevention applications. The system's development began at the request of a consortium of six of the leading banks in the United States. These banks met with SOFTPRO in March of 2003 to discuss the industry's need for an effective image-based fraud detection solution, and to formulate the requirements for such a system. FraudOne® has been created by SOFTPRO to meet those requirements and has been built from the start to be future-proof. The success of the platform has firmly established Softpro as a reliable partner with proven technology.

Trademark Information

- ✍ The following SOFTPRO products are registered trademarks in the U.S. Patent and Trademark Office or trademarks of SOFTPRO GmbH and/or its affiliates : FraudOne®, SignBase®, SignChip®, SignDoc®, SignInfo®, SignSecure® and SignWare®.
- ✍ Additionally the SOFTPRO GmbH holds additional national and international trademark registrations for its products SignCheck®, SignPlus® the product component Sival® and the company name SOFTPRO®.
- ✍ All other trademarks mentioned in this document are the property of their respective owners.