FRAUD FIGHTER™

Products by UVeritech

DOCUMENT FRAUD AT THE GOVERNMENT LEVEL

A WHITEPAPER DISCUSSING FRAUD PREVENTION METHODOLOGIES FOR GOVERNMENT AGENCIES

Opportunities abound for criminals to perpetrate “Document Fraud” against government agencies. Regardless of whether the fraud is in the form of fraudulent payment, or in the presentation of False Identity, these crimes have the capacity to cost government organizations $100’s of Millions every year.

SEAN TRUNDY, C.O.O., UVERITECH, INC.

CONTENTS

GOVERNMENT AGENCY FRAUD PREVENTION

Although most people may not think about it much, the many different levels of government, when considered together, compose the single largest transactional operation in the country.

Throughout the governmental hierarchy, from Federal, to State, County & City, at each level of government, facilities exist to manage the conduct of business with their relevant constituencies. Government agencies provide services and products to their "customers" – the citizens that fall under their jurisdiction.

Law enforcement, judiciary, utilities, records, licensing and permits – these are just a few examples of the day-to-day activities conducted between government and the populace that result in some form of transaction occurring. As we will show in this paper, anytime a transaction is conducted where some form of document is presented as a means to convey value of some type - or to purport a specific individual is who they say they are – fraud is a possibility.

Payment fraud is an obvious – and ubiquitous – problem confronting such transactions. The presentment of counterfeit currency, stolen or fraudulent checks or fraudulent credit cards poses a direct and immediate financial risk to government operations.

More recently, however, the advent of identity theft, and the use of counterfeit ID documents, has led to circumstances that concern governmental agencies charged with maintaining the security of our nation's airports, managing our Social Security network, and operating the nation's Medical Welfare programs. Such "ID-related" fraud costs the various levels of government 100's of Millions of dollars every year.

Solutions to the different levels and types of transaction that occur on a daily basis, across thousands of different locations, are many and varied. In order to make this document simpler and more focused, we elect here to focus solely on the prevention of document-related fraud. By that, we mean, those instances where fraud occurs as the result of an individual presenting a fraudulent document in the hope of obtaining value.

TYPES OF GOVERNMENT TRANSACTIONS EXPOSED TO DOCUMENT FRAUD

CURRENCY AND PAYMENT FRAUD

Some government agencies conduct operations that, in many ways, resemble those of private companies. Government utility companies sell power, water, and fuel services to their customers. County clerks' offices provide database and information services. Federal, State and County Courts receive filings, collect fees and penalties, and manage large quantities of data, all of which require payment through a cashier's office. The U.S. Military operate retail stores on their operations bases. Even prisons, to some degree, have retail operations and provide opportunities for prisoners and their families to make payments into prisoner spending accounts.

The centralized theme of all these operations is that, at some point, the customer must pay for the service or the good they are acquiring. Many such operations are, in fact, a straight forward retail-like operation, featuring a cash-register operator with a POS system. Payments accepted may include cash, credit cards, personal checks, money orders and debit cards or stored-value cards.

As has been seen in the private sector, where such payments are being made, the exposure to counterfeit fraud runs high. In fact, in some cases, the risk in these government operations is higher than it may be in private sector due to the perceived lack of security and preventative measures that may be present in the for-profit side of the economy.

ID DOCUMENT FRAUD

Identity fraud within the government transactional framework can occur in a surprisingly wide variety of instances. To properly discuss the issue, and possible solutions, it is helpful to segment this activity into sub-segments that can be classified and dealt with together. One possible method to segment this type of fraud is to consider the purpose for the presentation of a false ID document. Possible motives for committing ID Theft may include:

1. Theft of another's assets or records
2. To obtain access into a restricted environment
3. To claim benefits or other services belonging to another

Because of the different motivations that drive why an individual may attempt to present a false ID document, we find that a very large and diverse cross-section of government offices find themselves exposed to this type of fraud.

THEFT OF ANOTHER'S ASSETS

The concept is fairly straightforward. Under many different circumstances, a government agency may become the trustee or holder of an asset that belongs to an individual. In California, for example, the State Controller's Office becomes the holder of record of unclaimed life insurance benefits. The state publishes lists of such assets, which savvy criminals use as a source of potential leads. They can research who the next of kin might be, and then fabricate a set of identity documents for that person, including false driver license and birth certificate documents.

These criminals then can proceed to lay claim to another person's assets.

Other opportunities exist for this same scenario to play itself out at the State, Federal, County and City level of government. Customs and Border Control routinely seize shipments entering U.S. Ports. Law Enforcement often seizes assets during the course of an investigation. When a person's estate goes into probate, the court of jurisdiction will assume trustee rights over the assets in the estate. As previously mentioned, unclaimed goods are often held in trust by the state.

ACCESS TO CONTROLLED ENVIRONMENTS

Many government facilities are secured environments with restricted access. Military bases, U.S. Treasury buildings, Customs warehouses, Law Enforcement offices, airports, and Legislative offices and meeting rooms, to name a few, are examples of buildings in which access is controlled and restricted to specific personnel.

Criminals may seek access to such facilities for a variety of reasons. Not all such reasons are related to the theft of valuables. In fact, in most cases, the need to secure government facilities is a matter of national security. This means that, often, the task of securing the buildings falls under the control of the Department of Homeland Security (DHS).

The DHS establishes standards and controls designed to ensure that proper identity checks occur when screening individuals seeking entrance to their facilities. These checks can range from simple document verification, to document authentication and beyond to biometric scanning and facial recognition cross-checks against databases of known criminals.

CLAIM ANOTHER'S BENEFITS OR SERVICES

A third type of fraud enacted against government agencies involves the intentional misrepresentation of identity for the purpose of claiming another's benefits or services.

Every day in the Unites States, hundreds of millions of dollars of government services are consumed by beneficiaries of government programs. Medicare, Social Security, Veteran's Affairs, Food Stamps, government housing and a wide variety of other services and goods provided by the government to qualifying individuals are delivered to citizens, typically, based on the belief that an individual has established their identity.

> The Federal Office of Management and Budget (OMB) concluded there was about $125 billion worth of "improper payments" in 2010. This $125 billion included improper payments for programs including Medicaid, food stamps, unemployment insurance, Social Security and the school lunch program.
>
> politifact.com (2011-01-04)

Fraud through government programs is a massive issue. As the inset box to the right suggests, in 2010, it was a $125 Billion problem. While this huge amount was not confined solely to circumstances involving false identity documents, the fact remains that a significant portion of the fraud does occur when individuals present themselves under false identity. It follows, then, that putting controls in place to authenticate identity at the time that a benefit or service is authorized would serve to reduce this issue by a large amount.

DETECTING COUNTERFEIT INSTRUMENTS

Methods used by organizations for document authentication vary as greatly as the people who are doing the testing. The first distinguishing criterion is whether or not an external tool is used to aid them. Polls conducted by our company suggest that the vast majority of organizations do not, in fact, have specialized tools for this purpose, and require their transaction-level employees to perform document authentication using only their eyes, their knowledge and their fingers.

This, obviously, poses problems. Cashiers and tellers are often pressed for time as long lines of impatient customers demand they conduct transactions as quickly as possible. Add to this the vast array of different document types that must be verified, and the quantity of designs and styles that may exist, and it becomes clear that asking these people to accurately detect counterfeits – particularly counterfeits of high quality – is impossible.

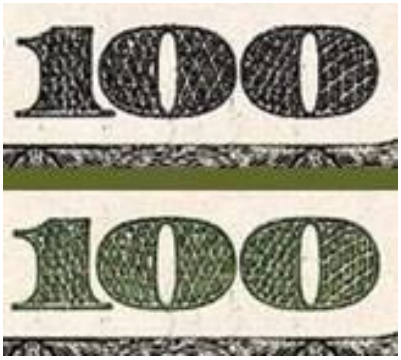
VISIBLE / PHYSICAL DOCUMENT INSPECTION

When conducting visible document inspection, the acceptor is attempting to verify that certain visible (or "overt") security features are present on the document. Examples of overt features include:

- Color-Shifting Ink
- Holographic Images
- Thermal Ink
- Intaglio Printing
- Watermarks

COLOR SHIFTING INK

Color shifting ink is a security feature that has been used on US currency notes since 2006. With the advent of the "big head" design, which began with the new $100 bill in that year, color shifting ink features have been added to each subsequent new bill design ever since.



Visual confirmation of this feature is quite simple. Look at the lower-right hand corner of the face of the bill, and notice the printed denomination numeral. Tilt the bill back and forth, thus changing the angle at which you view the number, and the color of the ink will "shift" from grey to green and back-again.

Color shifting ink is an effective, simple test that can be conducted easily by a cashier. As long as lighting conditions are good, this should be a valid technique to teach cash-handling employees. However, it should be pointed out that this feature has been compromised by enterprising counterfeiting operations, who have managed to replicate the general effect – in some cases quite well, and on other cases, with limited success.

HOLOGRAPHIC IMAGES

A hologram is an advanced-printing technique which creates the illusion of 3-dimensions on a flat (e.g. "2 dimensional) surface. Pictured below is an example of a hologram – as the viewer twists and turns the image, it will appear as though some colors are changing, and there will also appear to be "depth" in the image with some elements appearing to be in the forefront, while others appear to be further away, in the "back" of the image. The general theory behind utilizing them as a security feature is that they are difficult to copy, and that they are visible to the eye without the use of any equipment.

Holograms are commonly used on traveler checks, credit cards and identity documents. In the case of traveler checks and credit cards, the variety of different holograms is so small that a black market has sprung up in which excellent facsimiles of the holograms used by major brand names (e.g. Visa, MasterCard, American Express, Cook's, etc) can be purchased. Also, we have seen photocopies of holograms printed on metallic paper which can pass the very basic visual review.

Identity document holograms are typically of much greater detail and variety. Thus, they serve as a better source of security for such documents, PROVIDED THAT the person accepting the ID knows what to look for. We have seen websites in which fake ID documents containing very elaborate hologram features are included. If the teller or cashier receiving such a document doesn't have precise knowledge of the hologram as it should appear, then such a fake hologram can easily serve to fool even an attentive employee.

THERMAL INK

Thermal ink is an ink that alters when the temperature is changed. In the example pictured to the right, when the acceptor places their thumb on top of the keyhole image, the red coloring will disappear when the body heat increases the temperature enough. Once the paper cools again, the red ink will reappear.

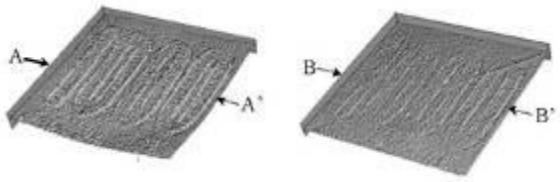
We have seen this type of security feature most commonly used on cashier's checks and money orders. We consider this to be a secure form of covert feature, since the technology to reproduce such features – while not advanced or difficult to emulate – does require specific chemistry and printing techniques typically beyond the counterfeiter. Thus, most counterfeit cashier's checks based on a template that utilizes thermal ink will often include the image of the feature, but it will not actually change under different temperature conditions.

INTAGLIO PRINTING

Intaglio printing is really the master overt defense for "printed" document security. Intaglio is a printing technique which utilizes intricately carved printing plates and extremely heavy printing presses to physically alter the surface of the paper that is

printed on. Very fine-details in the carved printing plates will cause ink to be forced into the fibers of the paper, creating a distinctive "raised feel" to the paper.

The image viewed to the left shows a high-magnification blow-up of a genuine intaglio-printed number "1000" (on the left) and an ink-jet printed "1000" (on the right). The genuine intaglio document shows just how clearly the ridges and edges of the numerals have been created. This is the result of the printing plates forcing the ink into the paper and causing the patterns to achieve a 3-dimensional aspect. The ink jet is not able to produce anything like this affect.



As a result of using intaglio technique, printers are able to produce very fine-detail in their printing. Consider this image of the US $100 bill. The very fine-line details both on Benjamin Franklin's face, and in the surrounding oval are produced at a level of resolution that an ink-jet or laser jet cannot match. Also, if one were to run their thumbnail along the fine lines, they would feel the ridges produced by the heavy-press.

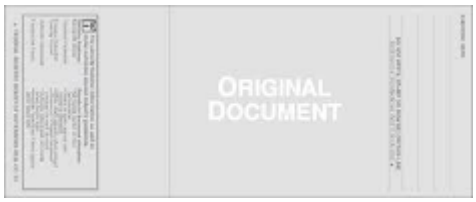
Because it is so difficult to reproduce both the resolution and the physical characteristics of intaglio printing, it is our opinion that, of all the "overt" features that can be used to verify documents – looking to authenticate the intaglio printing is the first-choice technique. This, of course, assumes that the document has intaglio printing.

WATERMARKS

Watermarks come in two general categories "genuine" or "artificial". Contrary to what these terms may mean in the context of a discussion on the topic of this paper, both these types of watermark are "real". The difference between a genuine and artificial watermark is how the watermark is created. In the case of a genuine watermark, a pattern or image is carved into a mold,

and the mold is used to "emboss" the watermark into the paper. That is, physically stamped in a technique that produces both a visible image and a sub-surface-level raised depiction of the image.

Artificial watermarks are really a type of replica or facsimile of a genuine watermark. In an artificial watermark, the mark itself is printed on the surface of the paper, but the printing is designed to make the watermark not easily visible unless viewed from an angle, or viewed with a light source held behind the paper (i.e. "backlit").



Watermarks are commonly used in currency notes. They are also found on most traveler checks, many types of cashier's checks and money orders, gift checks and more.

As a security feature, they are not very effective. Counterfeiters have found countermeasures – that is, methods to replicate the effect of a watermark – that are quite realistic. In fact, the "artificial" watermark method described above is available within some over the counter word processing or graphics programs. If used together with specialty inks, the overall effect of the counterfeit watermarks can be nearly indistinguishable from the real thing.

COVERT FEATURE DETECTION

Non-visible "covert" features are, by definition, designed specifically to not be visible to the human eye under normal conditions. For this reason, in order to verify the presence of such features, a tool or device must be used to enable the user to verify them. There are a number of different techniques for creating covert features. We will cover the following four "primary" methods in this document:

- Microprinting
- InfraRed
- Magnetic
- UltraViolet

MICROPRINTING

As the name suggests, microprinting is a technique in which extraordinarily fine detailed printing is performed on a document. In the case of US currency notes, microprinted

features are typically words printed in characters too small for the naked eye to see. As the example to the right shows, the newest design US $50 banknote contains several different areas on the note where different microprinted security features can be found.

Many of the world's major currency banknotes contain microprinted security. This second image is a sample of the $10 Australian banknote, which has microprinted characters smaller than 2mm in size.

In addition to currency, microprinting is commonly used to secure money orders and cashier's checks, and also, many different forms of identity documents contain microprinting.

We assess the security of microprinting to be relatively high. In order to achieve the very high resolution required to produce such fine detail, offset printing techniques must be used. This immediately eliminates the capabilities of a very high percentage of counterfeiters who are "digital artists" and do not have the skills or the equipment to conduct offset printing.

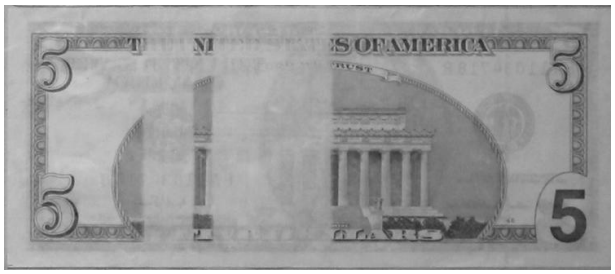
However, the issue from a retail/operational perspective is that performing a microprinting validation during a transaction is both intrusive and slow. The teller or cashier will need to use a magnifying glass or magnification imaging device in order to properly see the microprinting. This is a rigorous process. Meanwhile, the customer sees his ID or currency notes being scrutinized with a magnifying glass, and the "customer experience"- which is regarded as vitally important by so many organizations these days - is harmed.

INFRARED PRINTING

Infrared printing utilizes ink compounds that do not create any visible printed elements. By definition, "infrared" ("IR") is beyond the scope of human vision, so the inks used to print IR cannot be seen by the human eye. For this reason, in order to detect IR features, a device which is capable of rendering the IR inks into the human-visible spectrum is required.

This is typically achieved through the use of an imaging-scanner with an infrared lens. The lens "sees" the IR ink, and "translates" it into a black & white image that can be displayed on a viewing screen (LCD, LED, etc.). IR features are widely used on many different types of documents. Many world currencies secure their

banknotes using IR. Similarly, many national and international identity documents contain printing in IR inks.



IR printing is an effective security methodology. Printing with IR inks poses some challenge to the counterfeiter, although, with recent advances in digital printer toner technology, this has the capacity to become less of an issue. One of the true advantages of IR printing is its capacity to be rendered into "machine readable" characters or features that allow for automated validation by a machine, such as a bill acceptor on a vending machine, or a high-speed money counting machine. The image above shows the appearance of a US $5 bill under infrared light. The two "bars" are precisely located and can be easily "seen" and "read" by machines.

As a point-of-transaction security tool, we score IR to be rather low as an effective technique. The simplicity and ease with which a machine can validate IR features works exactly against the human employees that would need to verify the feature with their own eyes. Imagine attempting to teach employees how to distinguish between the $20 note, seen here, versus the $5 note previously pictured. In addition to the difficulty of training employees, the equipment needed to view these features is both bulky and expensive.

MAGNETIC CHARACTER PRINTING

Magnetic ink is used to print machine-readable characters that help automated devices to read and identify documents. These characters can be quite simple (e.g. dot-dash-dash-dot means a USD $5) or, they can be complex, such as the characters printed on checks (MICR) or on passports (B900) in which names, addresses, account numbers and other important information can be communicated.

At one time, magnetic printing posed a significant barrier to counterfeiters, however, this no longer holds as true as it used to. While it is still difficult to

produce complex magnetic features that can accurately recreate the B900 printing on passports (this information is encoded and requires decoding "keys" to be included), it is fairly easy to create the simple features seen on banknotes and personal checks. MICR printers are easily purchased through public websites.

Magnetic printing still offers a modicum of security on these simpler documents, due to the fact that many of the counterfeiters these days producing fake currency notes don't even bother to add the magnetic ink to their counterfeits. Thus, while conducting a simple "is there any magnetic ink?" test can detect some counterfeits, the fact that magnetic ink is present on a banknote or personal check by no means assures that it is genuine.

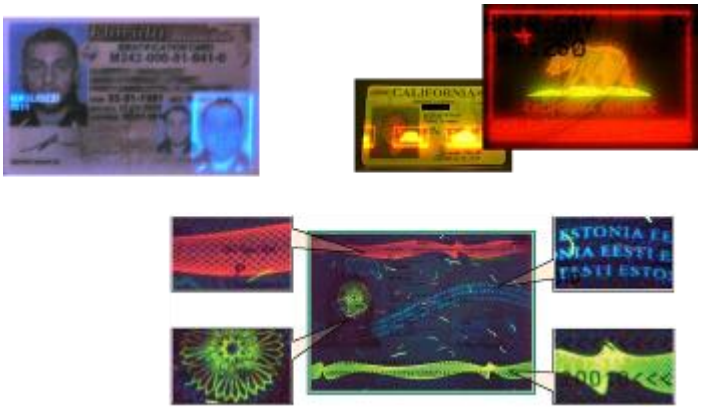
ULTRAVIOLET INKS

Similar to infrared, ultraviolet inks are designed to react to light sources that fall outside of the human visible spectrum. That means that the human eye cannot see the UV light needed to activate a UV security feature. However, the way ultraviolet ink reacts to UV light differs greatly from how infrared inks react to an IR light. UV inks, when excited by the proper wavelength of ultraviolet light, will produce a fluorescent response that is visible to the human eye, whereas the IR ink reaction still requires a filter or an imaging viewer to see the IR ink features.

Because of this capacity to "see" the security feature when it is properly excited, and, due to the fact that the UV ink is itself invisible under "normal" light, the use of UV security features has been widespread. Secure documents that contain UV features as a means to verify authenticity include:

- Currency notes (US dollars since 1996, most other world currencies)
- Passports
- National ID cards
- Credit cards
- Debit cards, stored value cards, gift cards
- Cashier's checks
- Traveler's checks
- Gift Checks
- Social Security cards
- Voting Cards
- Coupons (in some special cases)
- Casino Chips
- And more…

Printing with UV inks poses some technical challenges to the rank & file counterfeiter who use digital printers to produce their counterfeits. The compounds utilized to create UV fluorescence ("fluorophores") tend to be volatile – evaporating quickly unless locked into a neutral molecule (in US dollars, this is achieved by adding the fluorophore to the Teflon used to make the security strips embedded inside the paper). So, even if a UV feature is printed, it is likely that it will be only temporary in nature. In many cases, as with other covert security features, the counterfeiter either doesn't know UV security features exist, or chooses to ignore them completely, knowing that if they are patient, they can pass their fake documents in a location that does not test for UV fluorescence.



We rank the UV feature is being highly valuable as a security authentication method. In terms of its absolute security, it is not impossible to overcome the printing challenges, and some very professional counterfeiting operations have been able to replicate the features (e.g. "superbills" and government sponsored operations used to create fake ID's). However, the flexibility, ease of use, and relative low-cost of the equipment needed to enable UV verification at the point-of-transaction make it a viable option for use in many different situations – from small business to large enterprise.

SCIENTIFIC ANALYSIS

As we progress up the scale of accuracy and complexity regarding the manner in which documents can be authenticated, the third and final general category of technique leans more towards the "forensic" side of things. By this, what is meant is the examination of a document in a manner that compares known or expected values to what is observed or seen within the document itself. Examples of this type of document examination might include;

- Pattern Matching
- Machine readable zones/Data matching

These two concepts are based upon different authentication strategies.

PATTERN MATCHING

With pattern matching, the idea is that a document can be compared against a library of known features and designs to determine whether or not it is genuine.

Pictured here is a rendering, provided to us by L1 Identity Technologies, Inc. which shows the number and diversity of different security design elements that may be included in a single secure document design. This is not a comprehensive listing of such features, but rather, is an illustration that one document may contain dozens of individual design features that can be used in a pattern-matching application.

To verify the pattern of any given document, an intelligent library (database) is built that provides for a set of templates against which any document presented can be compared. Hardware devices then capture images of the document being tested, and those images are run through the database to identify, first, what type of document it is, and second, to determine what level of probability can be assigned as to whether or not the document is genuine.

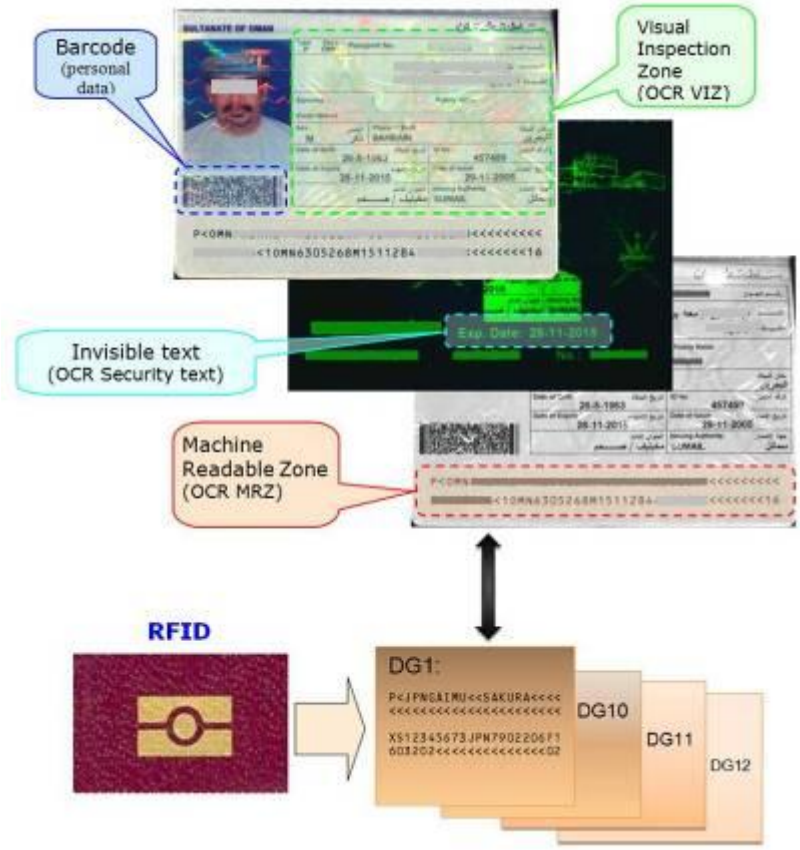
Almost by definition, the accuracy and reliability of this technique produces a very high level of confidence that counterfeit documents can be detected. The more complex the document (and the more complete the library used to match patterns) then the greater will be the probability of correctly authenticating a given document. So, for example, in some machines that look to verify currency notes, where only 3 or 4 elements are being examined, the accuracy level may be lower than other devices that validate ID cards ,which may have 20 or more elements to compare.

DATA COMPARE

The underlying strategy for how to authenticate a document using data compare fundamentally differs from that for pattern matching. With pattern matching, the

assumption is that "we know what the document should look like, so let's see if it matches". Data compare, on the other hand, is focused on gathering pertinent data from the document itself and comparing it to see if it all agrees with itself.

Multiple techniques are available to extract data from a document. Some we have already discussed, such as reading magnetic ink, or looking for identifying patterns printed in IR. We briefly touched on the idea of B900, which is an international (ICAO) standard format for printing machine readable zones ("MRZ").



Other techniques may include Optical Character Recognition ("OCR"), which is a software capability to "read" the printed information and translate it into a digital format. Advanced documents, such as passports and national ID cards may contain barcodes, magnetic storage media ("magstrips"), contact chips, contactless RFID chips and more.

After identifying the document type, "data compare" devices will first look to see whether all of the expected forms of data are available. Then, it will proceed to pull all of the available data and put it into a table so that the field content can be compared. Each of the above listed methods of storing data will have many fields that overlap. For example, "first name", "document number", "expiration date", etc. The software will compare the data from each of the different sources and make sure that they all agree. If discrepancies are found, the user interface will warn the user that there are problems with the data and the document may have been tampered with.

TOOLS FOR COUNTERFEIT DOCUMENT DETECTION

Available tools for counterfeit detection/document verification run the full spectrum, from the overly simplistic to the extremely complex. The choice of which is the right tool to use depends entirely upon the circumstances that define the exposure to fraud at each point of transaction. Not all transaction environments are alike!

In reviewing the types of device available, we have segmented them into two primary categories;

- Visible Verification
  - Microprinting
  - InfraRed
  - Magnetic
  - UltraViolet
- Forensic/ Machine Readable/ Pattern Matching Devices

The general division here lies between whether or not a "human decision" is required to make an authentication. The first category, visible verification, reviews devices that all require a person to make a determination that they "see" the proper security feature. The other category includes machines with software logic that tells you what they see, and do not necessarily require a person to make a determination themselves.

The following discussion is not intended to be a complete review of all possible products and devices, but rather, an overview of the types of device available which might provide the basis from which further research can be conducted by the individual reader.

VISIBLE REVIEW AIDS

These devices are designed to aid the user to see and verify the covert features that were discussed in the previous section of this paper. These devices do not have "built-in" logic to reach an authentication determination, but instead, rely upon the user to make a decision whether or not they see the appropriate visual clues to enable them to say that a document is fake or real.

MAGNIFIER/JEWELER'S LOOP

People can use a magnifier to view microprinting on documents. The "Jeweler's Loop" is a specialty type of magnifying glass used to look at documents.

Because microprinting requires advanced off-set printing techniques, many counterfeit documents either do not contain any microprinting, or the quality of the

printing is very poor and can be easily identified when viewed under magnification. In fact, the magnifier can be used to view any fine-line details that occur in higher-level off-set or intaglio printed documents. As the images to the right show, the genuine document (top) contains clear-to-see printing in the collar and very fine-detailed lines elsewhere, while the digitally reproduced copy (below) is unable to mimic these features accurately.

PRO's -- The advantages to using magnification are that the microprinting itself is a relatively high-confidence security feature. Only the most advanced counterfeits are able to reproduce such features that can withstand the scrutiny of a magnified review. Thus, if microprinting is verified, then it is quite probable that the document is genuine.

CON's -- There are several disadvantages to using this technique. Most importantly is the effect it might have on the "customer experience". There may be some environments where having someone bending over your document with a magnifying glass may NOT be offensive, but in most retail/hospitality/financial service circumstances, this would not be the case. Second, the teller or cashier really would need to know what to look for. In some cases, this may not be too difficult to train, e.g. if they were only required to review $50 and $100 bills. However, for ID authentication, or traveler check verification, they would need to remember a broad library of features. Couple this with the first point about customer experience, and the reality of using a magnifier at the transaction counter seems far-fetched. Finally, although they comprise only a small percentage of the counterfeits in circulation, there are some fake documents that DO contain appropriate micro-printed features. Specifically, these are documents produced in collusion with certain foreign governments. Thus, magnified review will not be able to detect these counterfeits

INFRA-RED VIEWERS

As discussed in the previous section when we explored the concept of infra-red security printing as a security technique, there are products available that allow a transaction-counter employee to view documents under infra-red light. Devices such as the one pictured on the next page use IR light sources to activate the IR

inks, and then an imaging display screen to render the IR ink imagery into black & white.

PRO's -- the advantage of IR ink verification is that most counterfeiting operations fail to include such features in their fake documents. Thus, if you know what to look for, and you actually see it, then, as with microprinted features, chances are fairly high that the item is genuine.

CON's – The greatest problem with verification of IR inks is the size and cost of the equipment needed to view the features. Devices such as the one pictured here can easily run $300-$500, and stand 18"-24" tall. Secondly, the features themselves are not "intuitive" or easy to remember. In the case of US Dollar notes, single or dual "bars" are visible, while on many ID documents, only certain parts of the text printed on the surface will be visible.

Ultimately, the IR ink features are better left to machines that are able to be programmed what to look for, and do not require the size or expense of an imaging screen in order to function. Many high-speed money counting machines and currency validators utilize IR ink testing as one method among several for identifying and validating banknotes.

MAGNETIC INK DETECTOR DEVICES

The idea behind a magnetic ink detector is fairly simple. Many secured documents are printed with "invisible" magnetic ink character-sets that can be decoded by devices designed to read them. This is commonly referred to as MICR (Magnetic Ink Character Recognition), and it is another technique commonly used by bill acceptors and high speed counting machines to be able to "see" and "identify" banknotes.

The concept of using this feature – e.g. – magnetic ink – as a technique to validate currency at the point of sale by a cashier or a teller is based on the belief that, if a device can detect the presence of magnetic ink on a banknote, then the bill must be genuine. Accordingly, numerous manufacturers have produced low-cost (as low as $5.95, in some cases) tools that can be manually traced across the

surface of a banknote, and when it detects a magnetic field, it will indicate, with a red light, or a tone or some other method to notify the user that it found a magnetic feature.

PRO's – The most obvious advantages to these devices are 1) the low cost and 2) the simplicity of the test. Rub the head of the tester around the banknote and look (or listen) for the indicator to tell you it is a good bill.

CON's – Unfortunately, the logical foundation behind the use of these devices is flawed. Everyone would like to think that a $6 tool can detect counterfeit currency, but the reality is that this test will do nothing more than detect counterfeits produced by absolute amateurs. As discussed earlier in this paper, in recent years, there has been a steadily rising trend of counterfeiters "washing" low denomination banknotes and reprinting them as counterfeit $50 and $100 bills. These "washed notes" commonly will have their magnetic features preserved, and thus, the user of these devices will receive a "false positive", indicating that the bill is genuine even though it is not. Also, a simple search of eBay or Amazon reveals dozens of vendors selling magnetic printers, and many of the major printer manufacturing companies produce magnetic ink cartridges for their printers. In addition, the "supernotes" produced by foreign governments do contain magnetic ink characters.

More problematic are the range of devices purporting to be "advanced" bill detectors, which do nothing more than give a "red" or "green" light to indicate whether a bill is false or genuine. These devices are, in fact, doing the same thing as the little $6 device pictured above, but they cost the user from $99 - $149 dollars!

UV LIGHTS

Ultraviolet lights are the final category of visible review aids, e.g. – devices that require a human to "see and decide" and which do not have any automated recognition logic built into them. As with the above three device categories, the general concept behind the use of a UV light is quite simple. Many documents are printed with special inks that only appear when they are viewed under the correct wavelength of UV light. The makers of such documents have placed the features there precisely so that they can be used as a verification technique.

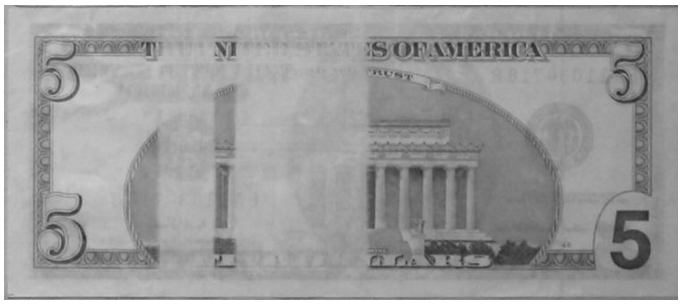
In the case of UV inks, the feature is entirely invisible unless it is exposed to the correct wavelength of UV light. Once this happens, then the feature "shifts" and becomes visible to the human eye, without the need for any additional tools. In this sense, UV inks really are designed as a "human readable" security feature, while some might argue that both IR and magnetic inks are designed to be machine-readable, only.

PRO's – There are a number of advantages to the use of UV as a tool for document authentication at the point of transaction.

- **Economical.** UV lights are among the lowest-cost solutions available in the market.
- **Simplicity** of use. Training of new employees is very easy. No complex set-ups or installations required.
- **Flexibility**. UV security features are present in an amazing variety of document types, from currency, to traveler's checks, credit cards, ID documents, casino chips, gift checks, cashier's checks and more.
- **Effectiveness**. UV inks have been an accepted method for securing documents for more than four decades, and continue to be utilized today by countries all over the world due to its high-level of security.

CON's – Disadvantages of UV lights are similar to those that pertain to the other visible verification techniques, namely, that it requires a human being to interact with the document and make a logical decision, i.e. – "Yes, I see the proper UV security feature". Many organizations do not wish to devolve this type of decision-making to the transaction level employee. Lack of proper training can produce confusion and inaccurate results. If an employee has not been told what to look for, or hasn't been provided with proper materials for reference, they could easily decide that they have received a genuine item when, in fact, it is counterfeit. One such example of this type of circumstance might arise in the case of a "washed $5 bill". This banknote – a counterfeit note printed on top of a genuine $5 bill – will show the "blue" $5 security feature when placed under a UV light. However, if it is a counterfeit $100 bill, this blue feature should be a dead giveaway, since the proper security feature for the $100 bill is "red". Improper training may lead to this type of event. A final potential issue with UV security features is that, while difficult to counterfeit, they are by no means impossible to reproduce, thus, it is possible that counterfeit documents can make it past this level of scrutiny.

Advanced analysis devices are those devices designed to pick-out and "read" the many different security elements placed into documents. In the previous sections, we have discussed IR ink, magnetic ink and UV ink printing as a means to provide "visible" verification. However, each of these printing techniques can also be utilized to create patterns, designs or characters that can be read by a machine and used as specific identifiers of a document type.



Referring again to this image of the $5 US banknote under IR light, the two "bands" seen here can be used as a basis for identification by an intelligent device, programmed with data regarding the location(s) & width(s) of this feature. Similarly, the IR features of the other denominations of US banknote would be programmed into the device.

Magnetic ink can be used to print actual characters which can be "read" by a magnetic reading device. Again, referring to a $5 bill, a magnetic reader would be able to detect and decipher the characters and would be programmed to know that these characters represent a $5 bill.

Other features, such as metallic threads, metallic inks, clear polymer windows, intaglio printing features and colors can also be identified by intelligent scanning devices as predictable and controlled attributes which can be read by the machine and used to identify the document.

MACHINE READABLE CHARACTER READING DEVICES

CURRENCY DETECTION

The marketplace has numerous devices designed to read Machine Readable features on currency notes to identify them as genuine. Buyers should be cautious before buying such devices that rely on only one type of MRC read. For example, those machines that utilize only magnetic ink, or look only at IR printing as a means of authentication. Instead, care should be taken to choose devices that test for multiple features and then cross-check the results to ensure that authentication will be reliable. Devices that read IR, Magnetic, UV, intaglio and other features in combination will be much more difficult

Bill Counter with Counterfeit Detection

for counterfeiters to defeat.

IDENTITY DOCUMENT DETECTION

Identity documents are also frequently provided with machine-readable information that can be used to identify them. These can be in many forms, including 2d bar-codes, magnetic tape, contact chips, RFID chips, digital watermarks, and more. While actual ID authentication requires a device that is capable of reading and comparing data from multiple sources, or looking at the details of the ID document itself, the MRC readers that function on ID documents will allow data to be read from the ID which can then be treated through software to achieve different results, such as age verification, visitor management, or maintaining records for compliance purposes.

DATA COMPARE DEVICES

Data compare devices take the concept of MRC to the next level. Unlike the previously described devices, which may read one or two Machine Readable data sets from a document, the data compare device will identify the document type (e.g. "California Driver License" or "€50 banknote"). The data compare software will know that on this document type, a given set of MRC data should be available. It will then look to extract that data, whether by reading basic printed features, more advanced digital security features, barcodes, RFID chips or whatever else may be included in the document.

By necessity, these are more complex devices that combine hardware and software. In some cases, as in currency authentication devices, they may be comprised of sensors and various light sources, while in others (ID authentication) the devices may include cameras, sensors, radio receivers, magnetic heads, and various light sources.

After extracting the available MRC data from the document, the device will build a table out of the data and "compare" the different sources to each other to make sure they agree. For example, the ID Reading camera pictured to the left can "read" the digital watermark on a driver license, decipher the barcode-encoded data, and/or perform an Optical Character Recognition (OCR) read of the information printed on the license. The software will then compare the different data points. Do all three sources give the same first name? Does the ID # agree? What about the date of birth, or the expiration date of the document? The results of this test will enable the software to determine a level of probability that the document is genuine.

PATTERN MATCHING DEVICES

Pattern Matching is a different sort of document analysis. Rather than reading data from the document and determining what it says, pattern matching attempts to determine whether the document itself is "built" properly.

In order for this type of device to work, knowledge of the advanced design elements of the documents it will authenticate is necessary. Thus, these tools tend to be focused on specific document types, and typically, on identity documents.

HYBRID PATTERN MATCH/DATA COMPARE DEVICES

The most successful and highly-accurate document verification tools typically combine some hybridization of the above-described techniques. These devices are developed in a manner that enables them to be used for more than just document authentication, but also for data extraction and storage. One example is the AssureTec ID150, pictured to the right. This hybrid device mechanically feeds a "DL-1" document (DL-1 is an international standard design used for driver license and national ID card formats). The ID150 reads bar-code and/or magnetic strip data from the ID document, then conducts some pattern matching tests (e.g. IR and microprint examination) to validate the document. It is able to extract data and images of the ID and will alert the user to any potential issues with the

document. To the left is a screenshot showing some of the results. In this case, the software was configured to alert for age-restricted product sales as well as for potential document authenticity issues.

Another device that fits this final category description is L1's B-5000 document authenticator. L1 Identity Solutions is the manufacturer of choice for the design and production of identity documents for the US government and 46 US state driver licenses. They also manufacturer a very large number of international ID documents. The B5000 is able to "read" ID1 documents, and passports and other global ID formats. Because L1 manufactures many of these documents, their pattern matching "library" is extremely robust. The B5000 unit is, in fact, a high-resolution camera which has built-in light sources that allow it to capture document images in IR, UV and white-light. These images are compared to its document library and high-confidence document authentication can be performed. This machine is also equipped with RFID and smart-chip readers to capture the information stored on them. The B5000 is capable of reading MRZ "zones" standard to ICAO document formats, and is B900 ink-capable. It can read mag-strip and bar-code data, and is also capable of conducting OCR reads of the printed information.

In other words, the B5000 captures almost every single element available on the document. It is then able to conduct a combination of pattern-matching and data-compare tests that allow it to authenticate the document. The results are highly accurate, and configurable so that a complete record of the document investigation can be saved to an encrypted file, including images of the document, and archived for later retrieval.

MULTI-LAYERED APPROACH TO FRAUD DETECTION

Addressing the multiple points of potential vulnerability to fraud loss and ID-verification related risks requires a systemic approach to risk analysis. Modern business organizations may involve diverse activities, including physical store operations, finance departments, "covered" financial transactions, sales of controlled products and acceptance of a broad range of payment types. Such activities must be evaluated with an eye towards scope, type and depth of risk at each point where the organization conducts a public-facing transaction.

Fraud Fighter™ believes a sensible approach to solving these mixed exposures to varied counterfeit transaction fraud and distinct opportunities for failed compliance with regulatory requirements is to construct an intelligently "layered" approach to the problem. Such an approach matches the features and functionality of the solution to the need at each individual point of transaction.

However, no solution can be meaningful if it cannot be purchased at a cost-effective price which provides a considerable return-on-investment. This is where the concept of "multi-layered" really achieves, because the goal of the solution is to place "tiered" security layers, with low cost solutions placed in those areas with lesser exposure, and only placing "high-end" equipment where the needs assessment determines it is imperative to have it.

MULTIPLE POINTS OF VULNERABILITY

No two organizations are alike. Even companies that are often compared to each other as "peers" will have unique requirements and varied exposure to different vulnerabilities. Similarly, no two points of transaction are the same. For this reason, it is not advisable to try to force an out-of-the-box solution to meet the needs of a company without first understanding what the problems and potential vulnerabilities are.

As an example, we could discuss the diverse operations of a large "grocery store" chain with whom Fraud Fighter has consulted and provided our solutions. Our initial understanding of the transaction environment was that this type of operation performed a high-volume of relatively low-value transactions with a transient customer base. On average, the stores operated 13 cash-wrap locations. Accordingly, the initial discussions driven by the customer were focused on the need to validate payment forms and to verify ID's for alcohol and tobacco product sales.

However, after learning in detail about the operations, we discovered that some of the greatest operational problems they had were associated with the "covered" financial transactions they conducted. Sales of money orders and electronic funds transfers to both domestic and international locations triggered a slew of regulatory compliance issues and reporting requirements. One Southern California region, alone, had seen greater than 25 separate IRS audits in one quarter in connection with the sale of money orders and wire transfer services.

In addition, the sale of PPA compounds (AKA, ephedrine, a pre-cursor chemical required for methamphetamine production) and the operation of a pharmacy also created the need to log and record identities of some customers.

In response, Fraud Fighter proposed a "multi layered" approach to address these vulnerabilities. At the cash-wrap locations, basic counterfeit detection devices (i.e. UV devices) were installed. At the customer service counter where money orders and wire transfers are processed, UV devices are installed alongside Image Capture devices to capture and securely store images of ID documents presented in order to comply with Red Flag, Customer Identification Program and Know Your Customer requirements. The same Image Capture device at the customer service counter is used to log ID's for purchase of ephedrine products. The Customer service desk also uses an electronic currency verifier to quickly scan high-denomination banknotes presented at the time money orders and wire transfers are conducted. At the pharmacy, a separate Image Capture unit is installed to log medical cards and ID documents for all purchases of Class I narcotics. Finally, in the back-office, the FF-1000 is used to quickly perform a double-check on cash-drawer reconciliation counts.

The "Displacement Effect"

This is a phrase Fraud Fighter coined after hearing the same observation from numerous customers. We have frequently found companies willing to address their "problem fraud stores" by placing our equipment into the stores where they are experiencing the highest levels of fraud. Afterwards, the LP staff would relate that problems in the stores with Fraud Fighter equipment had virtually disappeared, but the stores that previously had no problems were now showing signs that the criminals had focused their attentions on them because they didn't have Fraud Fighters. For LP managers who were given bonuses based on improved fraud numbers, those who had our equipment were at a distinct advantage over their peers!