UVeritech™

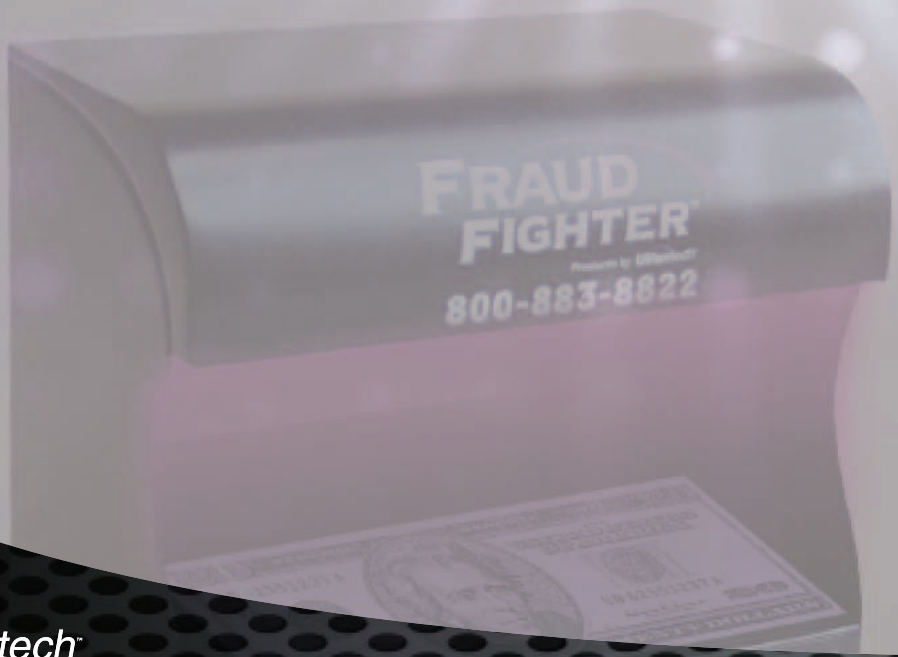
THE HOME OF FRAUD FIGHTER PRODUCTS

A Buyer's Guide to Counterfeit Detection Machines

How to Choose the Right Equipment for your Stores

- What type of documents do you need to authenticate?
- What is your budget?
- Do you need a permanent record of the transaction?

These are the types of issues you should consider before purchasing a counterfeit detection device for your business. – Sean Trundy



- Cash
- Credit cards
- Driver's licenses
- Identification cards
- Passports

Contents

A Buyer's Guide to

Counterfeit Detection Machines

Counterfeit Document Detection has become a necessary task within retail, banking and hospitality operating environments. The different methods used by organizations for document authentication vary as greatly as the people who are doing the testing. The primary distinguishing criterion dividing how organizations approach this issue 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. This implies that these organizations 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.

For this reason, it makes sense for organizations that conduct transactions with the public to consider installing equipment at the point-of-transaction to aid their employees in the task of identifying fraudulent payments and other documents which could lead to losses.

It is not surprising that a manager, business owner or loss prevention executive considering this issue may not know where to turn. For this reason, we have prepared the following buyer's guide as an effort to help focus prospective buyers' attention to the most important issues to consider.

Three essential considerations when choosing a counterfeit detector

What Type of Documents do you want to Authenticate?

For many people, the word counterfeit immediately makes one think "currency". Have no doubts, counterfeit currency is ubiquitous and can very quickly strike a company, causing tremendous losses. However, in the world of counterfeiting, almost any type of document that conveys value to the holder can be forged. As shown by real-world fraud statistics, driver licenses, coupons, traveler checks, credit cards, and many other important documents can be fraudulently produced and presented to your locations.

As a business owner or manager, you need to have knowledge of where your losses are coming from (or, where your exposure to such losses may be) and make a decision to purchase a detector that is capable of authenticating the types of documents that are important to you.

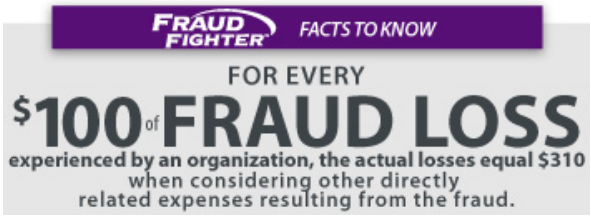
Do you Need to Maintain a Record of the Event?

Business goals that drive the decision to purchase a counterfeit detector will vary. In some cases, the goal is, simply, to deter potential fraudsters from attempting to present counterfeit items in your locations. If the bad-guys are not deterred, then the ability to detect the fraudulent item is a secondary benefit.

Other situations, however, may drive the need to actually log and record the event, and/or to maintain data that was derived during the authentication. Examples of this type of transaction might include sales of restricted items (like alcohol or cough medicines containing pseudoephedrine), or financial transactions that trigger compliance regulations under the Bank Secrecy Act.

What is your budget?

Of course, the budgetary question is overriding. Solutions are available for as little as $20, to as much as $4000+, depending on your needs. So, an analysis of costs, losses and potential savings must be conducted to determine where the sweet-spot - in terms of ROI - can be found. It is important to remember when conducting such an ROI analysis that the costs associated with the losses that result from fraud are not restricted, merely, to the dollar value of the fraud. In fact, extensive studies have proven that, ultimately, every $100 of loss that occurs as the result of fraud ends up costing $310 when additional matters, such as audits, investigations and other activities are considered.



Counterfeit Detector Types

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 wouldn't be offensive to the customer, 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

There are products available that allow a transaction-counter employee to view documents under infra-red light. Devices such as this one, pictured to the right, use IR light sources to activate the IR inks, and then an imaging display screen renders 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. 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.

U.S. Postal Money Order 2009

Dashed pink line.

U.S. Postal Money Order

Solid pink line with flourescent threads embedded in paper.

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

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 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

Bill Counter with Counterfeit 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 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 device pictured above can "read" the digital watermark on a driver license, decipher the barcode-encoded data, read data off a magnetic strip, capture data from an RFID chip 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.

Key consideration points

Ease of Use

We believe that the key to a successful new equipment roll-out lies in selecting equipment that is not more complex than it needs to be. While it can be easy to get sold on advanced features or functions, in the end, if you are looking, simply, for a device that can deter fraud and potentially detect the majority of counterfeits, then it may not be necessary to purchase a high-end device. Generally speaking, the

more functions and features there are, the more difficult it is going to be to introduce the product into your processes, and the more likely it is that installation will involve a myriad of departments, including IT, asset protection, and facilities management. For this reason, we typically recommend – go with the simplest solution that will achieve your goal.

Quality of Device

Quality is, in many cases, the primary distinguishing feature when comparing similar devices. In the case of UV lights, quality can be determined by a number of factors that are easily compared:

- Material – many low-cost UV lights made in China are constructed of low cost, brittle plastics and ABS materials.
- UV Power – Many UV lights are low-powered, utilizing only 4watts or less. Also, many low cost lights use improper electronics, so the bulbs do not operate according to their specification. Generally, a side-by-side comparison of lights will show drastic differences in how they are able to "fluoresce" the UV security features. Weaker, less costly lights will often be unable to cause red and yellow colored features to appear.
- General Design – When using UV lights, one is essentially looking for a "glowing" feature. This means, it is easy for that feature to be washed-out or hidden if your workplace is brightly lit by daylight or overhead lighting sources. Put another way, it is easiest to see a glowing security feature if the area you are viewing the document in is dark and shaded.
- Bulb Replacement - while this may seem intuitive, it is important that it be easy for store-level employees to conduct bulb changes. We have seen devices that require special tools and the skill of the craftsman in order to remove and install new bulbs.

Training & Customer Support

Once the product is purchased, you need to have materials that are able to easily teach your employees how to use the devices. What, specifically, do you want them checking? When do you want them to check? What should they be looking for when they do check?

This is one area where the quality of your vendor becomes the most important factor. Because your vendor should be able to design and/or provide unique tools for training that are specific to your needs. Do you need to verify traveler's checks? They should be able to give you resources for that. How about Driver Licenses? There should be an available guide for that purpose. In this way, your simple tool can become a powerful one.

Warranty and After Sales Service

I think everyone agrees that the true test of a vendor relationship doesn't occur until something goes wrong. At that point, you have a real chance to see whether your vendor values your relationship, or not. Manufacturers can brag about ISO certification, U/L listing, etc, but the fact is that sometimes issues arise with the product. What happens then? Will you be shunted into a voice mail system and never hear back from the vendor? Will you be forced into an "online customer service portal" which cannot answer your questions? Or, will you be able to speak to a real person and have your questions answered right away?