



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: [info@printech.com](mailto:info@printech.com) Web: [www.printech.com](http://www.printech.com)

# Document

YOUR GUIDE TO :

# Security



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: info@printech.com Web: www.printech.com

## FORWARD

### **Welcome to Your Guide to Document Security**

This booklet is designed to provide basic information that can be used to gain a greater understanding of the exploding issue of document fraud.

Document fraud is somewhat like the quiet plagues of the distant past. Banks were most often the victims and were quietly pushed into dark corners as falling prey to fraud was constructed as a limited problem. To the outsider, document fraud looked a lot like poor business practice or plain old irresponsibility. After all, how much could it actually be happening?

All that has changed. Fraud is a very big, very public problem. There are estimates that place the cost of fraud to American businesses somewhere between \$10 and \$14 billion dollars a year. In 1994, the American Bankers Association (ABA) made national news when they presented their findings on check fraud. The commercial banking industry estimated losses totaling \$815 million in 1993 with case loads up 236%. That's nearly two and one half cases every minute of every day. In 1990, the Uniform Commercial Code (UCC) was amended to change from the concept of strict liability on the banks part for fraud loss, to a shared liability situation driven by the relative responsibility for preventing the loss in the first place. Explosive growth in case volume and mounting losses compel banks to place greater responsibility for the prevention of check fraud on their customers. The revision to the Uniform Commercial Code may provide ample legal premise for the distribution of loss.

The public is increasingly being made aware of the costs associated with fraud of all types. It is a matter which virtually every business must acquire knowledge of and prepare appropriate defenses to avoid or reduce losses. For consumers, there are new challenges to understand the threats, the legalities, the risk and potential actions which must be taken.

*This booklet should in no way be construed as offering legal advice. Specific situations should always be reviewed with your own legal counsel.*

*Note: No right or license, expressed or implied, under any patent is created by the including of any security technique description in this document. The reader is cautioned to make independent inquiry as to such third party rights.*



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: info@printech.com Web: www.printech.com

## THREAT DEFINITION

Any discussion of document fraud needs to consider that task of identifying the threats to document security as they exist today and as they will likely exist in the future. All documents that have value or the potential to create value are subject to fraud. To limit the scope of this document to checks is a miscalculation of the nature of document fraud. It is certain that criminal techniques will evolve as defenses do.

### **Protecting Originals**

First and foremost in the need to protect access to genuine documents of value. Far too many instances of fraud are a result of negligent practices with regard to access to genuine documents or document processing equipment. The best way to commit document fraud is with a genuine document. Weak procedures to ensure protection serve as an open invitation to crime.

A part of protecting original documents is the need for an effective audit program. All items of value should be given a serial number of some type to permit reconciliation of lost or stolen items. It should be common practice to separate responsibilities within an organization. By this we mean that it could be construed as negligent to have the same individual write, sign and reconcile checks. In some cases, employers are deemed responsible for the acts of employees and a failure to provide for separation of duties contributes to the problem.

It should become common practice to protect any and all reference to account numbers and documents that can lead to unwanted access. All papers to be disposed of containing any reference to such information should be shredded as should any carbons that may contain confidential data. All packages containing valuable documents should be labeled with product code numbers and not descriptions such as "voucher checks" inviting unwanted access.

Lastly, for genuine documents, it is important to conduct periodic reviews of your security measures. Criminals will often take the time to understand your security program and attack at the point of weakness. For example, if your protective measures are implemented for items with a value of \$500 or greater, sooner or later you may fall victim to crime in the \$490 range. While one should not become obsessive about security, certain common sense protective measures are in order. There is little to gain by telling too many people every detail of your security measures.

### **Counterfeiting**

A primary threat today is the unauthorized reproduction of documents for unlawful purpose. This reproduction may take place via document scanners with computers, photo copiers, or illegal printing operations.

Desk top publishing software has created enhanced capabilities for the creation of documents that look quite similar to the real item. Current costs of scanning equipment, personal computers and laser printers have put this technology well within reach of criminals. For a mere ten thousand



dollars or less. The criminal scans a document into the system and can manipulate variable information creating output that can easily be used for fraud.

The color copier has evolved over the past few years into a device that is accessible to almost anyone. There are no particular skills required to operate a copier. This makes the color copier the single largest threat of document fraud today. If one lacks the money for purchase, there are lease options, or a trip to the neighborhood retailer where copies may be obtained for nominal fee. The color copier creates convincing duplicates. This opens the door to the casual criminal who otherwise would be deterred from such a practice. The presence of a color copier at a retail establishment provides greater mobility for the criminal.

There are a number of instances where members of a perfectly legitimate printing company have obtained access after hours to produce counterfeit documents. From time to time, one reads of clandestine printing operations that are established solely for illegal purposes. A printing operation requires far greater investment and expertise to put into operation than other methods of counterfeiting.

## Forgery

The alteration of a document for unlawful reasons is still a major concern. 66.7 billion checks were written and transacted in 1994. Suffice to say, they are accessible to the criminal. Two thirds of all checks written are used to pay bills. In the interest of "float," these checks are sent through the mail. This can be very secure and at times not. Consider how many times you enter a home or an office and there are stacks of bills waiting to go out. Or the criminal could easily go "fishing" in the neighborhood post box and obtain envelopes containing checks.

By washing or scraping information off legitimate documents, the criminal can alter such items as the "pay to" name to his or her own benefit. With automated deposits and document processing, there is little likelihood of being caught.

## DETECTION OF FRAUD

There are two issues that are fundamental to fraud detection. They are *detection of a fake document* and the *authentication of an original document*. Both are important aspects in combating fraud and every effort should be made to strike a balance of features to provide optimum protection.

Detection of the fake implies that there has already been a crime. The document has been altered or replicated. Certain features are designed to make replication more difficult to accomplish and visibly detectable by persons being asked to accept the document. Keep in mind that detection of a fake can be more difficult in many cases as the person being asked to accept the document has no idea what the original was supposed to look like. The ability to detect the fake is vital to the protection of persons who receive documents in good faith from unscrupulous types.



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: info@printech.com Web: www.printech.com

Authentication of the original is also difficult when one doesn't know what the document was supposed to look like. Authentication must be easily accomplished in a variety of environments to be effective. Key words like "safe" or "original" are useful but not fool proof. The goal is to create visible information that can be reasonably expected to permit a person to verify that the document is genuine.

## MARKET DRIVERS

There are many forces driving the explosion of interest in documents security. Most are the changes in technology, legislative and competitive forces that effect our daily lives.

### Technology

Ten years ago document fraud was largely a matter of forgery. The forger had the skills to alter documents in convincing fashion, such that they were easily passed. Simple forgery, while much easier to detect, was little more than a criminal signing someone else's name to a check. Still, the criminal was often successful and the bank absorbed the loss.

Counterfeiting was largely for the most sophisticated criminal as greater investment in equipment and skill were required. As a result, counterfeiting was mostly the illicit production of currency and credit cards.

Computing power has dramatically changed the picture. As referenced in threat definition, technology has become very sophisticated and very accessible. The fundamental breakthrough of computing power, the micro processor, has been integrated into many other devices greatly lowering costs and increasing counterfeiting capabilities. Desk top publishing and photo copier reproduction have made replication of documents, in quantity, a very simple proposition. The ease and accessibility have created an avalanche of criminal activity.

### Legislative and Judicial Issues

**It is important to note that this document should never be considered legal advise. Every situation must be reviewed for its own merit by an attorney.**

Persons that are engaged in the production, storage, or transportation of valuable documents must take reasonable care to protect these items from unauthorized access. A person or company that possess plates, films, work in process materials, or finished goods belonging to another must take reasonable care to see that these materials are safe from unauthorized access or be potentially held liable for loss resulting from unauthorized access.

There has been much discussion about the need for suppliers to make "security features" available to customers as protection against allegations of contributory negligence. The prevailing opinion is that a provider of documents having value should make all customers aware that security



features should be included in the documents but does not have a duty to include them if the suggested features are declined by the customer.

## **The Uniform Commercial Code**

The Uniform Commercial Code or UCC is a set of federal guidelines that are issued to reduce conflicts between individuals states engaged in interstate commerce. While not mandatory, code guidelines are usually adopted by each state in due course.

During 1990, the UCC was amended to reflect *ashared responsibility* stance in the area of check fraud. As of October 31, 1995, forty three states have adopted these revisions to the code. Prior to this change, the banking industry was held to *astrict responsibility* for losses resulting from check fraud. The code now specifically states that “persons or companies that are found to be comparatively negligent in the causes of fraud may be precluded from legal remedy in the recovery of loss.” Simply put, if a person or company can be shown to have been negligent, by act or omission, in that which caused the fraud, they may be subject to a sharing of the loss, or at a minimum may be precluded from legal remedy in the recovery of the loss.

The Code does not specifically define the aspects of comparative negligence. Rather, tests will take place within the court system on a case by case basis. The yardstick will be if a reasonable person would have been expected to take certain steps to prevent the crime but failed to do so. This will result in constant change to the concept of “reasonable” or “ordinary care.”

The practicality of the situation must be understood. A bank that has been hit with a substantial loss to fraud will have to examine the possibility of losing a customer they may have to sue to avoid the loss. There is strong likelihood that banks will more forcefully recommend various fraud prevention techniques to customers declaring that refusal to accept the suggested techniques may create a transfer for responsibility from the bank to the customer. Already a couple of such legal proceedings have been filed but were settled out of court.

## **BANKING ISSUES**

The banking industry is faced with mounting losses due to check fraud. Competitive pressures and the need to protect profits have and will continue to change U.S. banking procedures. The essence of fraud is very different from the banking industry’s point of view. They can only respond to that which they control. To that end, they must take every step possible to avoid the transfer of value to the criminal. This is best accomplished by placing a hold on deposited funds until such time as a document and an account balance may be verified. The problem is that criminals can move faster than banking.

### **Regulation CC, The Expedited Funds Act**

In 1990, regulation CC, The Expedited Act, was passed by the Federal Reserve. The act calls for banks to make funds available to depositors within two working days for local checks and within



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: info@printech.com Web: www.printech.com

five working days for non-local checks. The reality of the situation is that banks must make funds available by either the same day or the next day for competitive reasons. Depositors won't wait for access to their money. Banks that place holds on funds will chase depositors to banks who don't. The result of this pressure to make deposits more readily available mean greater access privileges by criminals.

## **Electronic Check Presentment(ECP)**

ECP is the transmission of check information electronically with the paper to follow. Banks involved in the transaction must be ECP participants. ECP permits information to be moved on a same day basis where it can be processed to verify the account balance. An invalid account results in a return item notice to the bank of first deposit and the funds may be withheld protecting the bank from loss.

## **Positive Pay Programs**

Positive pay programs are a fee service offered by some banks. The customer transmits an electronic check register each day to their bank. The bank will then reconcile every check received against the account to the electronic register refusing payment of any check found to be discrepant.

This service protects the bank's customers and keeps the bank from having to make hard decisions about how to respond to a loss suffered by one of their customers.

## **Imaging**

A technology on the horizon is "imaging." Simply stated, imaging is a picture of both the front and back of a check. This picture is created in a digital format rather than the traditional film and paper. As a result, check images require little storage space and may be transferred electronically. This will permit banks to curtail the movement of traditional paper documents and expedite the exchange of information for account verification purposes electronically.

Imaging will create a challenge for document security systems. Because images will be created in much the same manner as scanning or photocopying, there will be a need to create security features that will not interfere with the process. Reflective features like foils and holograms may present problems as will techniques that make or confuse the image in any vital check information area. Copy void features will produce "void" result when imaged. Certain colors of inks visible to the human eye will not be apparent during the imaging process.

## **CONSUMER AWARENESS**

Document fraud is an important issue. Consumer awareness has never been higher. At the end of 1994, The American Bankers Association(ABA) published their findings on check fraud. The story was featured in may newspapers and television broadcasts. Feature stories were carried by



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: info@printech.com Web: www.printech.com

CNN and NBC. Cover stories were spotlighted in Time magazine and U.S. News and World Report Magazine.

For American business, the topic has never been more important. The banking industry has gone public about a problem that is costing businesses millions of dollars per year. Their objective is to create public awareness and to notify customers that they may be held liable for losses not covered by the bank. The estimates for U.S. losses beyond banking are as high as \$14 Billion dollars annually. These losses do not include expenses associated with investigation, litigation, or lost customers.

## **F.S.A. Guidelines**

The Financial Stationers Association, or F.S.A. is a group of consumer check printers doing business in the United States and Canada. In 1995, the association chartered a task force to build public awareness of the growing check fraud problem. The reason for this desired awareness was, and is to preserve the checks as a viable instrument for the transfer of value.

The task force delivered a set of guidelines to be adopted by the members at large as minimum standards for security features on consumer checks. These features included a micro printed signature line, identified with a "MP" designation, a light screen on the reverse, and a padlock icon on the face (to the right of "dollars"). The padlock icon would direct the recipient to see the reverse of the check where security features could be listed. The padlock box used instead of a warning band.

In longer term, it is hoped that all checks will possess security features and that consumers will come to understand how to inspect and authenticate the document as "real." This will extend the life of checks as a way to transfer value.

## **FORMS INDUSTRY ISSUES**

The forms industry is maturing at a rapid pace. Participants will expand their businesses into new products or markets previously ignored, to replace declining revenues lost to alternative technologies or competitive pressures. This is evident by companies expanding into commercial printing, pressure sensitive labels, or advertising specialties to name a few. Secure document programs represent a product based opportunity for value added relationships and increased revenue.

There are several requirements for successful participation in the secure document business. They include but are not limited to such areas as education, marketing and adherence to some practical standards of performance. We will assume that you are pursuing educational needs by your use of this document.

Standards of performance for secure documents are those things a customer may never ask about unless there is a problem. Sadly, when they ask, it may be signal that the business is lost. Secure documents are, by their nature, confidential. Participants responsible for producing secure

document are expected to protect all elements of secure documents from unauthorized access. This includes all samples, films plates, production waste, and finished goods. Failure to protect materials from unwarranted access may constitute negligence, subjecting you to liability for loss, or at a minimum, the loss of a customer. Reasonable procedures in protecting secure documents from unauthorized access may be a marketable attribute today but will likely become a given very quickly.

## SECURE DOCUMENT DESIGN CONCEPTS

Over the many years that paper forms have been in use, people have learned those things that work will in the design and construction of a form. This is not necessarily the case in secure documents. There are a plethora of features that are all designed to deter specific threats. Like many security systems, the key is to optimize the level of protection and to select various features that complement one another.

### Layering

Think of layering as a system of deterrents that work together to provide greater protection. The concept of layering can be illustrated by looking at home security. The first and most basic layer is that you have doors and windows on your home that close and lock. The next layer may be lighting that is set on times or positioned to eliminate dark areas. Other layers may include dead bolt locks, security screens, bars, guard dogs, elaborate alarm systems and so on. The point is, layering should provide sufficient deterrence to cause the criminal to pass by the proposed target and go on the something that is less protected.

In document security, one would seek to combine complementary features that **are in** the paper, **on** the paper, or **applied to** the paper. This combination will be composed of covert (hidden) features which may be used to detect a fake or trap the criminal in the act, or they may be overt (obvious) features which are visible and may serve to authenticate an original or cause the criminal to select an alternate target. The need to balance the ability to detect a fake and to authenticate an original is critically important. There is value in each.

## PRINTED SECURITY FEATURES

A basic consideration of secure document design may be the printing technique that is used.

**Intaglio Printing** creates results that rise above (referred to as relief) the surface of the unprinted paper. This physical relief can contribute to the security of the document. Photo copiers can reasonably simulate intaglio printing by the thickness of toner on the surface of the sheet but the reverse will not reflect the recessed area under the printing that is physical with Intaglio Printing.

**Blind Embossing** may be an effective printing technique for security in that it does not use an ink. It raises the image above the surface of the paper. Blind embossing can be seen by the



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: info@printech.com Web: www.printech.com

human eye and can be detected by touch but is invisible to a copier. The reverse of this situation, debossing, may also be effective.

**Crash printing** that creates an embossed or debossed result is another example of a printing method that may be considered.

**Prismatic Printing** This technique may be described as the blending of two or more colors of ink in a single image. One ink tower is typically used and one plate. Inks are allowed to flow down the ink train to the printed image creating an effect similar to the way light blends through a prism. The resulting blend of inks challenges color copiers to simulate the original. The potential problem is that no two originals are exactly alike and unless you know what an original document looks like, the features may be less valuable. Like other overt (obvious) features, prismatic printing may suggest to criminals that there are other easier targets to pursue.

**Micro Printing** This is accomplished by producing an image that is smaller than can be read by the naked eye. Size may be about 1/100th of normal type size. While type this size can be easily printed, it is very difficult to copy or scan. The feature is covert and may be useful to authenticate an original by using a simple magnifying glass. Micro printing may be an image or a message.

**Secure Font Printing** A design aspect of security printing would be to utilize a secure font for type or numbers. A secure number font utilizes numbers that are different heights and widths so that efforts to cut a number and change the position of digits is very difficult. Imitation of the original technique is possible but less common. Secure fonts will not prevent replication of the document.

**High Resolution Printing** Printing of this type are called Guilloches. They are difficult to reproduce because they are produced at a higher resolution than copiers or scanners are capable of. Sophisticated computing techniques will permit resolution of this type to stay ahead of copiers for a while. United States currency is a prime example of such printing. Casual counterfeiters will find that high resolution printing will not copy or scan cleanly, resulting in muddy or inaccurate reproduction.

**Non-Repetitive Printing** This feature utilizes a different repeat pattern than the base document. The result is an image that is not in the same place on each document. In some cases a wavy line or "crazy line" is used and is printed in fluorescent ink so it can be used for verification purposes with a black light.

**Warning Bands** A key component of any security system is a warning notice that advises potential criminals that the document is protected. Like a sign that warns of danger, the warning band will serve to deter attempts at fraud. An effective warning message should be relatively simple to understand and difficult to remove from the document without harm to the printing nearby. The message should instruct a recipient to look for features that will authenticate the document. The absence of such features should cause the document to be unacceptable.

## **Copy Prevention Design Features**

Most common to copy design prevention features are embedded designs or messages. These covert features are intended to reveal a copy as a fraud.

**Void Pantograph** The void pantograph utilizes printed dots of differing sizes to create the effect. Smaller dots that are visible to the human eye dominate the appearance of the form. However, these smaller dots are lost in copying or scanning where larger less frequently printed dots become visible in the copy and spell out the word “void” on the face of the copy. Features of this type are very effective but may be challenged as resolution improves in copiers and scanners. .

**Wicker Feature** While delivering a similar result to the void pantograph, the Wicker technique is referred to as an “induced moiré effect.” Rather than vary dots by size and frequency, the Wicker technique utilizes lines of varied lengths and angles. This configuration is intended to create conflict with the scanning protocol of many machines. The resulting copy will be garbled and an obvious copy. Again, copier and scanner resolution improvements will challenge techniques like Wicker.

## **Reactive Inks**

Many different features can be built utilizing special inks. Reactive inks respond to light, heat, friction or chemicals. These inks are very popular for checks and currency in Central and South America.

**Fugitive Inks** This is a generic term that trends to be broadly used for various ink types. Basically, fugitive inks change by some inducement after it is printed.

**Metameric Pairs** These pairs of inks that look the same under certain lights, like incandescent, but look very different under other lights like fluorescent.

**Thermochromatic Inks** These are inks that respond to various levels of change in temperature. In some applications, human contact causes a color change or the color to disappear. Lower temperature inks sometimes return to their original color when the temperature change is removed. This technique is useful for authentication. Other thermochromatic inks react by changing color or becoming clear on a permanent basis. This can be very useful in instances where permanent evidence is needed to indicate exposure to the reactive temperature.

**Chemical Reactive Inks** These are inks that respond to the application of a specific reactive chemical. This chemical can be applied in many different ways. The ink will become clear or change colors on the document.

**Solvent Inks** Certain inks are made with very low pigment quantity. This creates a more transparent ink that is visible to the human eye but is not visible to a copier or scanner. The resulting effect is for the original to display a colored design or background that is not present on the copy. Further, the application of certain fluids will cause the ink to disappear.



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: info@printech.com Web: www.printech.com

**Fluorescent Inks** These inks are nearly invisible in ordinary light and very visible in ultra violet light.

**Infrared Inks** can only be read using infrared equipment

**Optically Variable Inks** that simulate iridescence or pearlescence can change color depending on the angle of light in which they are viewed.

**Phosphorescent Inks** lights up under ultra violet light and retain an after glow for a short period of time.

**Friction Reactive Inks** Some inks will rub or scratch off under friction, such as with the edge of a coin. Others will change color to reveal a more visible message. Both types can be useful to authenticate an original document. Either has appeal in that no special tools, ingredients or equipment are required to activate the ink.

**Bleed Through Inks** Inks of this type are often used for printing of MICR or serial numbers on documents. The inks contain a dye that migrates through the sheet of paper to create a reverse image on the back of the sheet. This image may possess color and is in exact registration with the image on the face. Bleed through numbers are effective prevention for cut and paste alteration and greatly complicate copying.

## PAPER FEATURES

Paper security features receive their classification because many are nearly impossible to produce if one is not producing the paper. Some features, like the chemical void, are actually added to surface of the paper after production by the paper producer.

**Anti Alter Patterns** Normally applied by a paper mill, this feature, sometimes called a weave pattern or laid lines, can be applied by a printer. The pattern makes cut and paste activity difficult to accomplish. The patterns are normally applied flexographic in pastel transparent inks. These inks will generally be difficult to copy due to their very low pigment content and high transparency. They will lose their color when certain fluids (like bleach) are applied to them. Patterns of this type are most common in safety papers. Patterns are considered to be low security because they are easily reproduced. Their value can be increased by applying them in exact registration front to back of a sheet.

**Ghost Features** A ghost is a feature that is visible when viewed at an angle but is more difficult to see in direct reflected light. Because copiers and scanners view documents from a right angle, a ghost is nearly impossible to replicate with a photo copier or scanner. Ghost features can be created using a variety of inks that range from varnish to various configurations of opaque or

transparent white. Ghost features are sometimes called artificial or simulated watermarks. Such a description is inaccurate and suggests the aspects of watermark security which is not the case with a printed device like a ghost. Ghosts are effective methods for authentication of originals and in limiting copying in photo copier and scanner environments. They can be easily duplicated by anyone who can print or by artists who may draw the design using white inks. For this reason, ghosts are relatively low security.

**Watermarks** True watermarks are of two principle types and can only be produced while the paper is being made and is still wet. They are pressed into the newly formed mat of fiber while it is still wet by a dandy roll. These are referred to as fourdrinier watermarks. The other type of watermark is cast into a mold creating much more intimate contact for an extended time with the fiber. The resulting mark is capable of remarkable detail and clarity. Watermarks of this nature are called cylinder mold watermarks. Each type is created on a different type of paper machine and it is common to speak of fourdrinier papers or mold papers. Watermark detail and visibility is obtained by varying the density of fibers in the sheet. This variation in density creates differences in opacity that yield the visual effect.

Watermarks are considered to be the most important security feature that has been created for document security. The security of watermarking can be explained in several ways. A watermark is very difficult to simulate (counterfeit) when it has good detail and clarity. This is accomplished by three dimensionality and tonal graduations that can be incorporated into the design. Furthermore, watermark security is greatly enhanced when the mark is recognizable by those asked to accept the document. Once a mark is recognizable, simulations become more difficult and detection can be easier.

Watermarks are very versatile in their use. They are visible in both reflected and transmitted light to the human eye.

Even though watermarks are easily visible to the human eye, they are virtually invisible to copier or scanner technologies. Reproduction by photographic or print methods produce distinctly different looking results. Simulation can be made even more difficult by creating watermarks that include light areas that graduate into shaded areas with great consistency. The more detail that can be built into a watermark the more easily a counterfeit can be detected. Watermarks can be made even more secure by creating custom marks that are proprietary in nature and are strictly limited to their owner.

**Chemical Sensitivity** Often referred to as “stain” features, chemical sensitivity is a key defense in the prevention of document alteration or forgery. Chemical sensitivity is designed to provide indelible evidence of tampering attempts on documents. It is a covert feature.

Such tampering is accomplished by washing ink off the original document and replacing the information with fraudulent data. Various fluids are used to wash ink from the documents surface. The type of fluid used will depend upon the type of ink used to write the document. For example, an oxidant like bleach would be used to wash a water based ink like fountain pen, from a sheet. Oil based inks might be washed off using various solvents.

There are several key considerations when selecting chemical sensitivity as a defense against fraud. Most important is to understand the various methods a criminal might use to forge the document. Second, one would want stain features that produce an indelible, easily seen stain that will cause the person who is asked to accept the document to look closer.

Many marketers promote stain features present in a sheet by reporting the number of stains. Effective document design will layer several stain features intended to respond to various chemical families to deter the criminal from attempting to wash off a stain to remove the evidence of tampering. For example, stain features that are designed to react to solvents may include a wide array of specific solvents that are a part of the solvent family. This may include mineral spirits, gasoline, toluene, and alcohol. All are solvents, but are they different stains? Our position is that stain families matter and that there are four stain families that constitute the marketing phrase “full chemical sensitivity.” They are the oxidants, solvents, acids, and alkalies chemical families. Certain other chemical types can be added but are usually specific to unique chemicals and are less common.

**Chemical Void** The chemical void is a printed message that usually reads “void” or “stop.” The message can be in any format or number of languages. While most often applied by paper manufacturers, the chemical void could be printed by most printers. It is printed in an invisible reactive ink that becomes visible when specific fluids are used to wash ink off the document. Most chemical voids are designed to react to oxidants like bleach, but other chemical reactions are possible. The covert feature is intended to give further evidence of tampering and does not restrict photo replication in copiers or scanners.

**Visible Fibers** Fibers are added to paper to make replication of the document more difficult. These fibers are visible in ordinary light and can be of various colors, lengths and densities. By putting an array of fiber colors into the design that are different than the printed image one can greatly complicate counterfeiting by making it necessary to print many extra colors. Color copiers that use toner, can duplicate fibers, but the created image will be on the surface and detectable to the touch. True fibers are imbedded into the sheet and are not bumps on the surface. Also, because fibers are added when the paper is being made they generally are present on both sides of the document. Careless counterfeiters are likely to ignore the need to copy the back as well as the face. Using fibers as an overt (obvious) feature will signal the criminal that the document is protected and perhaps, deter fraudulent attempts.

**Invisible Fibers** While invisible in ordinary light, this covert feature is most often responsive to ultra violet (black) light. When the document is placed under black light the fibers become quite visible. Like fibers that can be seen in ordinary light, invisible fibers can be added in an array of colors, lengths and densities. The inclusion of color makes simulation a much more difficult procedure. Because fibers are invisible, they are not intended to restrict photo copy replication. The copy however will not contain the fibers and can be quickly detected by viewing the document in ultra violet light. Invisible fibers are a very effective layer that completes a comprehensive security system.



**Planchettes** Planchettes are available in visible colors, fluorescent visible colors, invisible fluorescent colors, iridescent colors, and fugitive colors. These small discs are slightly larger than the head of a pin. They are embedded into the paper during production of the paper and normally do not rise above the surface. Planchettes can be registered in narrow bands or dispersed randomly in the sheet. Planchettes are more effective when multiple colors are used. They may be one or two sided.

Like visible fibers, a selection of visible colors can greatly complicate counterfeiting. Invisible fluorescent colors are effective in verification as they can be viewed under ultra violet light. Like visible colors, iridescent colors are effective for authentication providing extra security in that they change color when viewed at differing angles.

Fugitive colored planchettes are thermochromatic in nature. Heat causes the planchettes to lose its color, becoming clear. Once the heat is removed the color returns. This is an excellent verification method in that no tools are required beyond the heat of human touch. Simulations using toners or non-reactive inks will not have the same performance.

Planchettes represent an effective security feature that can be overt when visible planchettes are used or covert when invisible planchettes are used.

**Hi Lites** Small particles are added to the paper to create HiLites and may be visible colors, fluorescent visible colors, or invisible fluorescent colors. An array of colors optimizes the effectiveness of this feature in visible and invisible formats.

**Security Threads** Security threads are polyester or plastic bands that are embedded into the paper. Threads generally are just beneath the surface of the sheet. This restricts visibility in reflected light while permitting good visibility in transmitted light. Security threads offer protection against photo copying because copiers and scanners see documents in reflected light. Security threads resist copying and scanning most effectively when they are mini or micro printed as the printed message is most often illegible on the copy. Security threads are an excellent overt feature. The presence of the thread in a document will provide for easy authentication.

There are many optional features that can be added to threads to enhance their security. In some cases threads can be made to serpentine from the middle of a sheet to the surface and back to the middle. Threads of this nature are referred to as windowed threads. Security threads can be miniprinted (legible without magnification) or microprinted (legible with magnification). They may be metalized to create a bright metallic appearance. They may be magnetic responsive. They may be created with a hologram effect. They may be printed in fluorescent colors to make them react to ultra violet light. Threads can be of varied widths. While it is possible to put threads into fourdrinier papers, windowed threads are only available in mold papers.

**Erasure Sensitive Coating** These are coatings that are intended to provide evidence of attempts to erase or scrape information from a document. The first type is a layered coating of white over a color. An attempt to erase or scrape will cause the top white layer to come off the sheet



8402 NW 64 Street, Miami, FL 33166 Tel.: (305) 592-2838 Fax: (305) 477-7540  
E-mail: info@printech.com Web: www.printech.com

revealing the color making the attempt visible. The second type has microcapsules on the sheet with a reactant that forms color when the stock is tampered with.

**Toner Adhesion Coating (Toner Lock)** Documents that are imaged by laser can be altered by removal of the toner from the surface of the document. To increase the difficulty of such alteration, toner adhesion coatings are added to the paper to cause the sheet to be torn or damaged indicating tampering. These coatings are covert in nature and do not restrict photo copying of the document.

**Instant Verification Features** This covert feature is designed to provide for authentication on an original document. A chemical is applied to the paper that will respond to a specific reactive ink. The ink is used in normal transactions by stamp pad or pen and creates a colored mark that authenticates the document as an original. After marking with the special ink, the absence of a color reaction would indicate that the document is a copy.

**Iridescent Coatings** Primarily used in currency, these coatings are added to the surface of the sheet in patterns or type. The coated area will change color when viewed from differing angles. This overt feature may be photo copied to create a counterfeit but the duplicate will be a single color when viewed from any angle and the iridescence will be lost.

## CONCLUSION

The most effective document security program is multifaceted, one that layers procedures and features together. Procedural security is important to lessen the chances of an "inside job". Valuable documents and account information should be protected from unauthorized access as should document execution equipment. There should be a separation of responsibility between those who execute valuable documents and those who are auditing them. Without secure procedures, security features have little value.

Security features will bring you peace of mind and provide you with the best chances to avoid the losses that come from fraud.

This document is brought to you courtesy of Appleton Papers