DOCUMENT SECURITY AND AUTHENTICATION
Introducción

Los documentos de valor pueden describirse como cualquier documento, más allá de las notas de banco, que se puede utilizar para generar dinero, identificación, acceso o la creación de documentos de identificación. Estos pueden ser impreso por muchos procesos modernos como: offset, flexográfico, gravure, digital, silk-screen y intaglio.

- Código Mercantil Uniforme 1
- Control Corporativo 2
- Cómo Mucha Protección Necesitas 4
- Documentos no Financieros 5
- Los Desafíos 5
- Los Objetivos 6
- Enfoque Integrado 6
- Incentivos para la Contratación de Contrabando 6
- Incentivos para la Contratación de Contrabando 7
- Client/Forms Profesional/ Fabricante 7
- Inks Anti-Replicación de Seguridad 8
- Capas de Seguridad 11
- Appvion’s Full Line of Security Options 12
- Análisis de Riesgo WhitePaper 13
- Documento de Seguridad WhitePaper 18
- Resumen 20
THE UNIFORM COMMERCIAL CODE

The UCC is the longest and most elaborate of the uniform acts. The Code has been a long-term, joint project of the National Conference of Commissioners on Uniform State Laws (NCCUSL) and the American Law Institute (ALI),[1] who began drafting its first version in 1942. Judge Herbert F. Goodrich was the Chairman of the Editorial Board of the original 1952 edition,[2] and the Code itself was drafted by some of the top legal scholars in the United States, including Karl N. Llewellyn, William A. Schnader, Soia Mentschikoff, and Grant Gilmore.

The Code, as the product of private organizations, is not itself the law, but only a recommendation of the laws that should be adopted in the states. Once enacted by a state, the UCC is codified into the state’s code of statutes. A state may adopt the UCC verbatim as written by ALI and NCCUSL, or a state may adopt the UCC with specific changes. Unless such changes are minor, they can seriously obstruct the Code’s express objective of promoting uniformity of law among the various states. Thus persons doing business in different states must check local law.

The ALI and NCCUSL have established a permanent editorial board for the Code. This board has issued a number of official comments and other published papers. Although these commentaries do not have the force of law, courts interpreting the Code often cite them as persuasive authority in determining the effect of one or more provisions. Courts interpreting the Code generally seek to harmonize their interpretations with those of other states that have adopted the same or a similar provision.

In one or another of its several revisions, the UCC has been enacted in all of the 50 states, as well as in the District of Columbia, the Commonwealth of Puerto Rico, Guam[3] and the U.S. Virgin Islands. Louisiana has enacted most provisions of the UCC, with the exception of Article 2, preferring to maintain its own civil law tradition for governing the sale of goods.

Although the substantive content is largely similar, some states have made structural modifications to conform to local customs. For example, Louisiana jurisprudence refers to the major subdivisions of the UCC as “chapters” instead of articles, since the term “articles” is used in that state to refer to provisions of the Louisiana Civil Code. Arkansas has a similar arrangement as the term “article” in that state’s law generally refers to a subdivision of the Arkansas Constitution. In California, they are titled "divisions" instead of articles, because in California, articles are a third- or fourth-level subdivision of a code, while divisions or parts are always the first-level subdivision. Also, California does not allow the use of hyphens in section numbers because they are reserved for referring to ranges of sections; therefore, the hyphens used in the official UCC section numbers are dropped in the California implementation.

ORDINARY CARE

Just What Is Ordinary Care?

Here is the technical definition: “Ordinary care in the case of a person engaged in business means observance of reasonable commercial standards, prevailing in the area in which the person is located, with respect to the business in which the person is engaged.” Still, what does ordinary care mean to business owners? The answer is this: among other things, Ordinary Care is a group of responsibilities, or controls, that business owners must exercise to fully demonstrate that they have taken reasonable action to safeguard their company's checks. There are six controls that will help assure that Ordinary Care is being exercised. In a moment, we will examine those responsibilities in detail. But first, let's look at another important facet of the revised UCC: Comparative Negligence.
COMPARATIVE NEGLIGENCE

Prior to the revisions in Articles 3 and 4 of the UCC, if both the bank and the customer were found negligent in a check fraud case, the entire loss would be placed upon the bank. Now, however, under revised Articles 3 and 4, the principle of Comparative Negligence is introduced. Comparative Negligence basically means that both parties can be found liable for check fraud. How much depends on their relative degree of negligence or fault. Here’s the definition of this concept: “Comparative Negligence requires the allocation of loss between the parties when both are negligent or when both have failed to exercise ‘Ordinary Care’. The Comparative Negligence rule leaves it up to a trier of fact (a jury or a judge in a non-jury case) to reach something of a mathematical formula in allocating liability.” And here is an important point to consider: under revised Articles 3 and 4 of the UCC, the burden is on the customer to establish that the bank failed to exercise Ordinary Care.

SECURITY FEATURES AND ORDINARY CARE

What Is The Role Of Security Features In Exercising Ordinary Care?

Legal experts agree that security features could well become an important aspect of Ordinary Care in the future. Brent Gorey, an attorney who specializes in the banking industry and the legal aspects of checking, says: “I believe that, in appropriate cases, a strong argument can be made that the failure by a business to use security features to protect its check constitutes negligence.” According to the legal publication, The Law of Bank Deposits, Collections and Credit Cards: “one form of customer negligence that is beginning to attract attention is failure to use state-of-the-art security features in check paper stock. If ABC Corporation could have used check stock with proven anti-forgery security features, but failed to use it, ABC has to that extent failed to exercise Ordinary Care in preventing the check forgery in the first place, particularly under revised UCC Article 3-406. Given the wide variety of check security features now available to companies at reasonable prices, it is foreseeable that this ‘state of the art’ defense will start appearing in check cases.

Can My Business Really Lose Money To Check Fraud?

In a word, the answer is “Yes.” Thieves are becoming increasingly sophisticated, and at the same time, the banks, bolstered by revised Articles 3 and 4 of the UCC, are taking a tougher position regarding check fraud.

SIX CORPORATE CONTROLS FOR CHECK SECURITY

By implementing the following controls, business owners can greatly minimize their exposure and risk to check fraud. These controls, among other things, help demonstrate that Ordinary Care has been taken to protect a company’s checks.

Control #1: Examine Bank Statements Promptly

It is essential to exercise reasonable promptness in examining bank statements. Here is an important rule: let’s say a situation occurs where a company’s checks are used illegally because of a forged signature. If the bank establishes that the company failed to exercise reasonable promptness in examining its statement, and if the bank establishes that it suffered a loss because of that failure, the bank has no liability so long as it acted in good faith and was not negligent. Here is another important rule commonly known as the “Repeater Rule”: the rule takes force when a bank customer does not report a forged signature and the same thief forges a signature on additional checks paid more than 30 days after the first forged check or bank statement was made available. In this case, the bank has no liability on the additional forged checks so long as it acted in good faith and was not negligent. More importantly, the bank does not have to establish that it suffered a loss.
Control #2: Report Losses Promptly

Just as it is important to promptly examine bank statements, it is equally important to quickly report to the bank any unauthorized payments due to forgeries or alterations. Regarding prompt reporting of a problem, here is an important rule: bank customers are obligated to discover and report a forged signature on their checks within one year. If they fail to make the discovery and report it to the bank within one year, they are barred from making any claim against the bank. This rule applies even if the bank was somehow negligent.

Control #3: Maintain Adequate Security and Controls

One of the most important steps any business owner or executive can take is to assure that company checks are maintained in a safe and secure manner. Some of the safety steps include the following:

- Company checks should be kept in an area that is secure and locked, with access limited to those individuals with responsibilities for issuing checks.
- To maintain strong security, it is recommended that the keys or combination locks that safeguard the checks be changed on a regular basis.
- Always keep check boxes sealed until they are required for actual use.
- Mechanical signing equipment should be kept in a secure area away from blank checks.

Under Articles 3 and 4 of the UCC, if a bank customer is negligent in adequately securing company checks, and if that negligence substantially contributes to a forgery, the bank will in many cases have no liability.

Control #4: Segment Check Responsibilities

To minimize the odds of check fraud, it is important that different people within an organization have responsibility for check functions. For example, one person would be in charge of maintaining check stock custody and preparing checks for signature while another person would reconcile the monthly bank statements. The following rule underscores the importance of minimizing check fraud by dividing check responsibilities: revised Articles 3 and 4 of the UCC provide that if an employer entrusts an employee with responsibility to sign, endorse or deposit checks, and if the employee forges the endorsement of the employer on a check payable to the employer, the endorsement is effective if it is made in the name of the employer. The bank does not have to establish any negligence on the part of the employer. So long as it acted in good faith and was not negligent, the bank is not liable for the forged check, and the check customer will be responsible for the financial loss.

Control #5: Institute Controls Over Accounts Payable and Payroll Functions

Another important deterrent is to have appropriate controls over the accounts payable and payroll functions. Only authorized personnel should be allowed to add or change vendors to the company’s computer system. Controls should be in place to insure that only legitimate employees can be added to the system.

Control #6: Conduct Periodic Audits

It is important to conduct periodic audits of the various check control functions. This will help make sure the overall system is working as it should be.
How much protection do you need?

Take this simple test.

As a general rule, the more checks you write the more risk you have. The same holds true for value bearing documents like coupons and certificates. To help gauge your level of risk, take this simple test.

Enter your score for each question in the box. Select one answer only per question.

1. How many checks do you write per month?
   - 30 or fewer.................................................................+1 point
   - Between 30 and 100..................................................+2 points
   - Between 100 and 300.................................................+4 points
   - More than 300..........................................................+6 points

2. Do you write checks to people or businesses you don’t know?
   - Rarely (maybe once a month).....................................+1 point
   - Sometimes (3 to 5 times per month)..........................+2 points
   - Often (5 to 10 times per month).................................+3 points
   - Frequently (more than 10 times per month)...............+4 points

3. Where do your checks get cashed or negotiated?
   - Almost always in my home state................................+1 point
   - Sometimes out of state..............................................+2 points
   - Often out of state....................................................+4 points
   - Usually out of state..................................................+5 points
   - Sometimes in other countries...................................+6 points

4. What’s the value of the checks you write?
   - Almost always less than $250....................................+1 point
   - Mostly less than $500...............................................+2 points
   - Mostly less than $1000..............................................+3 points
   - Frequently more than $1000.................................+4 points

Add up your TOTAL SCORE .........................................................

How did you do?

Use this table to determine the DocuCheck® Security Product best for your needs:

<table>
<thead>
<tr>
<th>Total Score*</th>
<th>4-5</th>
<th>6-8</th>
<th>9-11</th>
<th>12-14</th>
<th>15 or higher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Level</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>DocuCheck Product</td>
<td>Basic</td>
<td>Ghost</td>
<td>Impede</td>
<td>Watermark</td>
<td>Custom</td>
</tr>
</tbody>
</table>

* If you’re between levels, move to the next higher risk category.
NON FINANCIAL DOCUMENTS

Aside from traditional checks and money orders, there is a wide scope of printed documents that have become targets for counterfeit attack. Birth certificates can be used to create new identities as well as secure additional identification documents such as a driver’s license and social security number. Fraudulent marriage licenses can be used to bring illegal aliens into the country as well as gain access to government agencies for money or services. Labels are counterfeited putting low quality products into the supply chain which may create damage to a company brand as well as put that brand in a liability situation. Badges and other credentials can allow someone access to a location or database which can be used for many forms of criminal activity.

Counterfeit products currently represent a predicted value of over $750 billion dollars globally with over $250 billion within the USA in brand product alone. From checks to clothing, permits to certificates, coupons to wine labels, counterfeiting of printed documents has a large impact on our daily businesses.

THE CHALLENGES

Document fraud is one of the largest challenges facing financial institutions, businesses, governments and document security printers today. The ever-increasing sophistication of low cost technology makes it easy for today’s criminal to produce near perfect counterfeit and altered documents. With complete computer systems, that include a color scanner and printer, selling for under $1,000 and US sales of color copiers jumping from 40,000 in 1994 to over 200,000 today, you don’t have to be a professional printer to turn out quality documents.

Document fraud is a growing problem that is not always taken seriously. Not until federal legislation was enacted in 1998 did assuming another individual’s name and identity become a federal crime. Still today, not all states have laws prohibiting the theft and subsequent use of another person’s social security number, credit history or checking account. Now, this federal crime will carry hefty penalties and restitution requirements.

Key statistics are showing an ever-increasing fraud growth rate:

- A 2013 study by the Association for Financial Professionals reported that 61% of organizations surveyed experienced attempted payments fraud with a typical loss of more than $20,000.

- A 2012 survey by BankInfoSecurity found that check fraud is the second most common fraud scheme and that 76% of banks ranked check fraud among the top threats they face.

- Large organizations were significantly more likely to have experienced payments fraud than were smaller ones. (93% of all respondents)

- The most prevalent reason why an organization does not use a particular fraud prevention service is cost/benefit does not justify its use (36%).

- Checks were the dominant payment form targeted by fraudsters, with 93 percent of affected organizations reporting that their checks had been targeted.

- According to the Document Fraud Institute, “Each year, U.S. companies lose more than $600 billion to fraud, with ‘counterfeiting and document fraud’ making up more than two-thirds of that.”

- Approximately 11.7 million persons, representing 5% of all persons age 16 or older in the United States were victims of one or more types of identity theft within a 2-year period. (Department of Justice (2012)
THE TARGETS

- Checks/Vouchers – Any organization issuing checks or payment vouchers runs big risks of counterfeiting and tampering, and multiple levels of document security features are a must.

- Parking Passes/Stickers – Counterfeits can cause loss of revenue and even liabilities if forgeries are used to gain access to unauthorized areas.

- Product Labels – Fraudulent labels on counterfeit products can flood a marketplace and expose consumers to inferior product presented under a company’s brand name, thus damaging the true product’s brand image.

- Tickets or Coupons – Event tickets or retailer coupons can often be easily counterfeited with obvious potential loss to the event venue or store.

- Medical Documents – Prescription forms and other sensitive medical documents are also potential targets for counterfeiters.

- Insurance/Financial Documents – Many documents in these industries contain sensitive personal information and should be secured against tampering or reproduction.

- Government and Legal Documents – Government entities and other official organizations need to secure printed documents such as permits and licenses, birth/death certificates, vouchers, authentication documents and certificates of origin/titles. Risks include loss of revenues and damage to consumers.

- ID cards and Personal Identity Documents – It’s critical that issuers use state-of-the-art document security techniques to protect any documents containing sensitive personal information. ID cards, birth certificates, passports and related documents are among the favorite targets of thieves.

THE SOLUTION

INTEGRATED APPROACH

With the appearance of low cost, high-definition laser color scanners, printers, and copiers, the attention previously paid to forgery (the illicit alteration of a document with the intent to deceive), has been refocused towards counterfeiting (the illicit reproduction of a document with the same intent).

It is realistic to accept that given time, resources, and inclination, the integrity of any document can be compromised. A secure design advocates collective defensive elements as part of an integrated approach to document protection that involves design, printing technique, security ink and security paper to discourage fraudulent activity. The various component elements can be made to reinforce each other's effects to provide enhanced security on any document.

DETERRENTS TO COUNTERFEITING

When included at the design stage, security devices offer mutually protective elements that tend to resist counterfeit or forgery more effectively than by simply adding a security feature to an already existing document. Keep in mind that not all such designs are aesthetically pleasing.
Anti-duplication defenses whose function it is to prevent an acceptable copy from being made, accentuate some
deficiency in a copier or scanner’s response to duplication of all colors in the visible spectrum. The appearance of the word “VOID” on the copy of a document is a good example of a deterrent
design device. Experience shows that some colors reproduce stronger than ideal above a
certain density, but weaker below it. This observation has generated ideas for designs that tend
to photocopy with an exaggerated contrast. The more distinguished cause “VOID” to emerge
from its cleverly camouflaged background when the document is photocopied.

Because color copies and scans are composed from lines of colored dots arranged in strongly directional
patterns, some designs are intended to provoke Moiré patterns. Moiré is a phenomenon incurred when critically
spaced parallel lines intersect a small angle with the scan lines from a copier or scanner. Obtrusive Moiré fringes
will appear as patches of distorted colors.

By contrast, the concepts offered by paper and ink manufacturers involve the appearance or disappearance of
some key feature rather than an image. Some are authenticity devices that are present on the genuine
document, but the effect is absent from a photocopy. Paper-based examples are watermarks, security threads,
fluorescent fibers or planchettes. Ink-based examples are heat-sensitive thermochromic ink and optically
variable ink, whose perceived color changes according to the viewing angle.

Ink manufacturers also offer visible and invisible luminescent materials, sometimes with a dual wavelength
feature; penetrating watermark ink, UV activated photochromic inks, infrared pairs, metameric pairs etc. Some
inks, like watermark and optically variable, are overt in the sense that the eye alone readily
identifies their presence or absence. Heat-sensitive thermochromic inks change from color to
colorless or color to color, then reverts back to the original state, usually within seconds. These
overt effects can not be photocopied. Other inks like luminescent and infrared need special
authentication equipment to detect their presence so they maybe described as covert. In all
cases a knowledgeable inspection is necessary because both overt and covert features may
themselves be counterfeited. The inappropriate choice of a readily available security device
may lead to a very real potential for deception by a fake document. To provide greater
protection we encourage the use of more than one security feature on each document.

**DETERRENTS TO FORGERY**

Only a coordinated approach involving a combination of good design, fugitive inks and sensitized paper will offer
adequate protection against forgery. Forgers have adapted a wide range of chemicals for the fraudulent removal
and alteration of signatures, endorsements and variable information. Household bleaches, disinfectant, dry
cleaning fluids, hair spray and a host of other chemicals in the hands of skilled criminals have the potential to
remove laser toner, and ballpoint pen, marker pen, ink jet, and stamp pad inks etc. Obvious targets for forgery
are documents such as checks, vital records, gift certificates and passports.

Chemically sensitive papers usually respond to falsifying chemicals by the appearance of a color stain, and
fugitive inks will bleed, stain and dissolve on the printed document. Fugitive inks also have the versatility to
protect an entire document or only that portion that needs protection. Both sets of responses are designed to
deter the forger, or betray his attempts. Superficially, the devices are similar, and in an economic or competitive
environment where price is the prime consideration, a choice between paper and ink will inevitably be proposed.
A proper marriage of security ink and security paper affords mutual protection, and allows a far surer defense
than is possible separately.

**CLIENT/FORMS PROFESSIONAL/MANUFACTURER PARTNERSHIPS PAY OFF**

Today’s successful security document forms professionals are providing their clients with an approach to
document security that offers multiple levels of protection, including overt and covert measures. These
professionals understand their customer’s documents of value and their life cycle. They know how the documents should be designed, focusing on the vulnerable areas of attack. The professionals work with their customer to understand the verification environment and propose the best authentication feature available for their surroundings. The successful distributors are using a common sense approach of being proactive, not reactive in offering their clients the latest technology in document fraud protection.

Like all business situations, the decision to use security defenses to protect a customer’s document from counterfeit or fraud is not a simple one. The decision depends upon a fine balance between economics and performance, the printer’s capability and the client’s needs. It entails the involvement of various industry technologies from a vast array of suppliers that can include software companies, paper manufacturers, ink suppliers and others. The distributor and customer should understand how each vendor’s involvement might impact the ultimate effectiveness of a document’s defense and consult each supplier candidly. The confidential nature of this undertaking requires working with manufacturers to ensure maximum effectiveness of the document’s security. Once a decision is made to integrate security defenses into the product mix, it is important for the distributor to illustrate for the customer how the additional marginal costs of building an effective, secure document are offset through the improved, secure document.

**USING INKS TO SECURE DOCUMENTS OF VALUE**

Ink plays an important role in preventing document fraud. As a security feature, ink can be utilized as covert or overt protection to secure a document from unlawful duplication and alteration. It has the versatility to protect an entire document or only that portion of the document that needs protection. Ink can provide a means to instantly authenticate a document by something as simple as human touch or as sophisticated as machine-readable devices. Unlike other security devices on the market today, ink security can easily be built into the design of a document utilizing conventional printing processes.

**ANTI-DUPLICATION SECURITY INKS**

**COIN REACTIVE**

Coin Reactive ink offers instant authentication for many types of sensitive documents and is available in two offset versions, opaque white or transparent white. Opaque white coin reactive ink is commonly used to print an overt watermark on uncoated substrate where the printed text or logo will become more apparent under two different stimuli. First, the print will appear gray when rubbed with the edge of a coin or other metal object and second, the same print will appear with a swipe from a highlighter pen. The transparent version is printed covertly and usually in a discreet location on the document where criminals are most likely to use razor blades to fleck or scratch information off laser printed checks and gift certificates. When the printed area is violated by the razor blade, gray smudge marks will appear making the attempted alteration apparent.

For additional document protection, Coin Reactive inks should be employed with other security inks on the same document.

**FEATURES**

- Opaque white or transparent offset versions
- Simple to verify with a coin or other metal object
- UV fluorescence can be added, providing additional security to the document
- Coin Reactive effect can not be photocopied or digitally recreated
- Offset - Opaque white and transparent
- Flexo - Opaque white
BLEACH REACTIVE

Bleach Reactive inks are designed to give a chemical reaction between the colorless print and a solution of weak bleach, one of the more frequently used counterfeiting agents. The print changes irreversibly to a brown color. Since it is colorless, it is virtually undetectable until bleach or other strong oxidizer come in contact with the printed document. The ink is used mainly as an authenticity feature for printing invisible “Void” patterns on sensitive documents, especially on checks.

For additional document protection, Bleach Reactive inks should be employed with other security inks on the same document.

FEATURES
- Covert ink feature with strong overt evidence of chemical attack from bleach solutions
- Irreversible color change
- Bleach Reactive effect cannot be photocopied or digitally recreated
- Offset

INFRARED INVISIBLE BLACK

Infrared Invisible Black ink provides an ink-based security feature for many types of sensitive documents. This ink is rendered invisible when viewed through an infrared image viewer.

For additional document protection, Infrared Invisible Black ink should be employed with other security inks on the same document.

FEATURES
- Clear proof of document’s authenticity
- Invisible effect cannot be photocopied or digitally recreated
- Offset and flexo

METAMERIC

Two inks that appear similar in color under one set of light conditions but have appreciably different optical properties under another set of light conditions. These matched ink pairs provide an excellent method to conceal hidden words or logos used in a printed background. The hidden word or logo can only be detected through a special viewing filter. Metameric ink pairs are best color matched on the press.

For additional document protection, Metameric inks should be employed with other security inks on the same document.

FEATURES
- Concealed word or logo easily verified with special viewing filter
- The covert effect is difficult to photocopy or digitally recreate
- Secondary security ink feature of UV invisible fluorescence can be added to ink “B”, the ink that is used to print the hidden word or logo
- Offset

NUMBERING

These security-numbering inks contain a component that penetrates red dye into the paper’s fibers that show through to the back of the document. It is almost impossible to lift the numbers from the paper surface without
authenticate a document by something as simple as human touch or as sophisticated as machine-readable Offset - Opaque white and transparent Coin Reactive effect can not be photocopied or digitally recreated

ANTI-DUPLICATION SECURITY INKS

Ink plays an important role in preventing document fraud. As a security feature, ink can be utilized as covert or overt. When rubbed, this heat-activated ink will change to a colorless state or to another color. Then within seconds the ink will revert back to its original color. Document authentication is as easy as rubbing the printed area between two fingers to trigger the color change. Thermochromic ink is an excellent security device to authenticate a genuine document from counterfeit.

Two types of color changes are available, color to colorless and color to color. While various activation temperature ranges are available, T25 (Color appears at 72°F and becomes colorless at 90°F) and T35 (Color appears at 81°F and becomes colorless at 90°F) are SICPA’s standard activation ranges.

For additional document protection, Thermochromic inks should be employed with other security inks on the same document.

FEATURES
• Simple to verify with human touch, no special devices needed to authenticate document
• Color changing effect is impossible to photocopy or digitally recreate
• UV invisible fluorescent or photochromic marker can be added as secondary security features
• Offset, flexo, gravure and screen

UV FLUORESCENT

Single UV fluorescent and dual UV fluorescent inks fluoresce under ultra-violet (UV) light. Single, long wavelength (360 nm) ultra-violet fluorescence is commonly used by itself, printed invisibly, or incorporated into another type of ink, i.e. fugitive, numbering, thermochromic or conventional inks. Dual ultraviolet wavelength invisible fluorescent ink; fluoresces one color under short wavelength UV (250 nm) and another color under long wavelength UV (360 nm) is less common.

For additional document protection, UV fluorescent inks should be employed with other security inks on the same document.

FEATURES
• Easy to authenticate document with UV light source
• Undetectable under normal light conditions
• UV fluorescent effect is impossible to photocopy or digitally recreate
• Offset, flexo, gravure and screen

SECURITY COATINGS

DESENSITIZING

Transparent spot-applied ink, which will deactivate selected areas of the CF surface of carbonless papers. Desensitizing ink works by desensitizing the Lewis acid of the phenolic resins or clays, which are the main components of the coating of the CF copying paper.

FEATURES
• Use with other security inks for enhanced document protection
• Contains fluorescent marker to check printed coverage on press
• Offset

TONERBOND™

Invisible toner adhesion ink used to prevent the alteration of laser imprinted documents. TonerBond™ is most effective when spot printed in vulnerable areas of a document on non toner bonding based substrates.

FEATURES
• Applied to at-risk areas of a secure document to prevent lifting of laser imprinted toner image
• UV invisible fluorescent marker has been added to aid the printing process
• Cost-effective alternative to fully coated toner bonding substrates
• Offset
### All Attributes

**DocuCheck Basic**
- UV Dull
- Invisible fibers
- Three chemical stains
- Optional Toner Fuse

**DocuCheck Ghost™**
- UV Dull
- Artificial Watermark (AWM)
- Invisible fibers
- Three chemical stains
- Optional Toner Fuse

**DocuCheck Impede®**
- UV Dull
- Linemark
- Invisible fibers
- Three chemical stains
- Optional Toner Fuse

**DocuCheck Watermark®**
- UV Dull
- True Watermark
- Invisible fibers
- Five chemical stains
- Optional Toner Fuse

**DocuMark® Custom**
- UV Dull
- Custom Watermarks
- Visible & Invisible fibers
- Chemical sensitivity
- Pen Tick Plus™
- Authentication
- Machine readable features

### All Security Feature Descriptions

**Invisible Fluorescent Fibers:** Only visible under ultraviolet light; can’t be photocopied or scanned.

**Chemical-Reactant Stains:** Full (High-Polarity Solvents, Low-Polarity, Oxidants/Bleaches, Acids, Alkali): Reacts with these chemicals to readily show tampering.

**Artificial Watermark:** Low level security feature; ghosted visual patterns are easily duplicated by counterfeitors.

**Crosshatch Pattern:** Low level security feature; many of these papers are available to criminals “off-the-shelf”.

**Toner Adhesion Coating:** Locks toner into the paper; resists forgery.

**LineMark™:** Lines optically change from dark to light depending on the reflected or transmitted light; this feature helps to make DocuCheck® Impede the best medium-level security paper available.

**Visible Fibers:** Resists scanning; authenticity verification.

**True Fourdrinier Watermark:** Shows a negative image in reflected light and a positive image in transmitted light; DocuCheck Watermark® is unique in its clarity and definition.

**Chemical-Reactant Stains:** Partial (High-Polarity Solvents, Low-Polarity, Oxidants/Bleaches): Reacts with these chemicals to readily show tampering; DocuCheck® stains remain even after 60 minutes underwater.

**Duplex Color:** Front white (ANSI Standard X9.7 compliant); back white, blue, green, pink, or tan; deters duplication. Color disappears where exposed to bleach (fugitive color) to deter alterations.

**UV Dull:** Low reflectance in UV light; won’t interfere with fluorescent printed features and optical reading.
RISK ANALYSIS IN DOCUMENT SECURITY: Assessing and Defending Against Potential Threats.

Counterfeiting is increasing at dramatic rates and targets are more widely varied than ever before. Any company issuing documents of value, documents of identity or using product labels may be potential targets for counterfeiters.

Universities, insurance companies, government agencies (vital records, titles, permits, licenses, etc.), park and wildlife organizations, wineries and other manufacturers, financial institutions, and brand owners of all types need to protect their printed documents, labels, stickers, marketing materials and more from the attacks of counterfeiters. This represents a tremendous opportunity for print distributors and resellers, who can help clients protect their businesses, their customers (i.e. personal identification documents), their customer relationships and their overall brand image through document security techniques designed to deter unauthorized reproduction, copying or tampering.

DETERMINING THE RISK – WHERE TO START

Document security risk analysis is a process involving a series of probing questions designed to identify past, present and potential future attack methodologies against a company’s printed documents. This is a critical process that must be undertaken in depth to best ensure that recommended solutions offer a strong defense against the particular document fraud risks of a given client. All departments of a company that could be impacted by counterfeit attacks must be included in a thorough risk analysis and interviewed for their insights into the problems they are encountering and their ideas on prevention. This could include sales, customer service, legal, returns/repairs, marketing, production and possibly other departments.

A SENSITIVE SUBJECT: PREPARING TO ASK THE TOUGH QUESTIONS

There’s no way around it. Some difficult questions must be asked to create a risk analysis that will yield any true value. When conducting a document security interview, the print reseller needs to be mindful of the sensitivity of the subject. You will be probing deeply into sensitive areas about a company’s products and services, as well as their handling of brand image, corporate reputation and their current principles of document protections. Individuals who carry responsibilities directly related to these subjects may feel threatened by your inquiries, and great care needs to be taken to depersonalize your presentation to avoid damaging personalities or raising concerns of personal job security.

It’s your job to help them see past all this, and realize their input will ultimately help drive better document security solutions, which will protect the company as a whole, and also yield benefits to them personally, although it may be indirectly.

BUILD FROM THE BOTTOM UP

Once you have reached an agreement with management to conduct a risk analysis, it is often helpful to conduct interviews for a document security risk analysis starting from the “lower tiers” of a company’s organizational structure, and then working your way up to interviewing executive management. The questions will tend to build upon one another, and the higher up the hierarchy of command and responsibility one goes, the more a given manager will have influence over key factors. To help you assess the ideal hierarchy of which departments to interview in which order, think of the pay levels of ground level employees within given departments. For example, it may make sense to begin with the customer service and production departments, then work your way up the ladder to marketing and sales, then legal and executive management.
Whatever order the interview process unfolds in, it makes best sense to do executive management interviews last, as you will have increased knowledge of potential issues related to counterfeit attacks on the company. When interviewing executive management, all of the questions should be asked, dividing each segment of the interviews into sections by each department category of impact (i.e. “let’s talk about the impact of counterfeit attacks on customer service and production…now let’s talk about how it could affect marketing…sales, etc.”). This will cause executive management to focus on how all encompassing a counterfeit attack could be on the company, and help them to more fully appreciate the potential damages and costs associated with legal ramifications, employee and customer relations, marketing and brand image, and most importantly…sales revenue.

IDEA INSIGHTS

- Checks/vouchers
- Tickets
- Permits
- ID cards
- Certificates of origin/titles
- Parking passes
- Coupons
- Licenses
- Birth certificates
- Passports
- Product labels
- Medical documents/prescription forms
- Insurance/financial documents
- Authentication documents
- Personal identification documents

DOCUMENT SECURITY RISK ANALYSIS: QUESTIONNAIRE

This is a basic guide to performing a document security risk analysis, with a series of potential questions that could be asked of all departments with a direct or indirect connection to the repercussions of document security attacks. You may not need to ask all of these questions of all individuals, and other queries will naturally come up in the flow of this process, but be sure to probe as deeply as possible with each pertinent interviewee.

Interviews at the executive level should include each section of questions below, making sure the executive participants focus on the particular discipline within the company for each section of questions. After taking executives step by step through the questions focused on each department under their charge, the interview will conclude with final questions which are specifically focused on executive level concerns.

INTRODUCTION:

Explain why you are there, and the risk analysis process in which they will be participating. Cite the various departments and personnel you will be interviewing, and the importance of each participant’s role in helping maximize the benefit of the document security risk analysis. Take steps to comfort each individual as to the proprietary nature of their responses, assuring them of your respect of confidentiality if they are concerned about sharing information they feel could threaten their position.

Define the types of documents potentially at risk from counterfeit attacks, give examples of the potential impact of these attacks, and an introduction to some of the possible solutions to defend documents against counterfeiting and alteration.
RISK ANALYSIS QUESTIONNAIRE

WHAT TYPES OF DOCUMENT SECURITY OR COUNTERFEIT ATTACKS, IF ANY, HAVE YOU SEEN AGAINST YOUR COMPANY’S PRODUCTS OR SERVICES?

❑ Were any of these attacks targeted at altering any of your important physical documents?
❑ Do any of these attacks involve your customers’ sensitive personal identification information?
❑ Were any of these attacks focused on mimicking your brand, producing inferior “knock-offs” with fraudulent labeling?
❑ What would you say is the most prevalent attack that has or is occurring with any frequency?
❑ What would you say is the most damaging of these attacks?
❑ Do you foresee any weaknesses or areas that are open to potential attack but have not yet been exploited?
❑ Do you have any ideas for addressing these issues and defending against future attacks?

WHAT HAPPENS TO YOUR DEPARTMENT WHEN A DOCUMENT SECURITY OR COUNTERFEIT ATTACK OCCURS?

❑ What percentage of your department’s time is currently dedicated to dealing with issues related to document security or counterfeit attacks?
❑ How does an attack affect your normal duties?
❑ Would it negatively impact your ability to take care of customers?
❑ Would it negatively impact your ability to take care of your regular internal responsibilities?
❑ Could time lost dealing with these attacks negatively impact overall performance in your department?
❑ If attacks were reduced or stopped could your department serve internal and external customers more effectively?
❑ What percentage would you attribute to an increase in performance, if any, should your department not have to dedicate time to deal with document security or counterfeit attacks?
❑ Do attacks cause direct or indirect labor costs within your department?
❑ In terms of real dollars related to your department, what would you estimate these attacks cost the company?
❑ Following an attack, do you feel employees may question the stability of the company?
If employees were to have doubts of the company’s stability, could these feelings be passed along, either intentionally or inadvertently, during daily communication with customers?

What impact would it have on internal communications if employees were to have doubts of the company’s stability?

How could employee compensation at your company be impacted if less time and money were spent managing the effects of an attack versus selling?

**CUSTOMER SERVICE AND SALES DEPARTMENTS**

**WHAT IMPACT DO YOU FEEL DOCUMENT SECURITY AND COUNTERFEIT ATTACKS HAVE ON CUSTOMER RELATIONS?**

Would customer perception of the value of your products/services be damaged?

Could an attack cause customers to worry about the reliability of your other products and services, given the attack on one of your lines?

How likely do you think customers would be to look to other suppliers or brands for their consumer choices?

Would an attack create an additional workload within your department?

Would an attack create additional phone traffic for your department?

Could an additional workload or increased phone traffic caused by an attack lower employee morale within your department?

**RETURNS & REPAIRS DEPARTMENT**

**HOW DO YOU CURRENTLY AUTHENTICATE RETURNS?**

If your department were inundated with counterfeits would employees be aware they were repairing or receiving fake products?

How would you handle requests for repair or returns on counterfeit items?

What would be the potential costs to repair or replace counterfeit items, both per unit and per the potential overall scale of a counterfeit attack?

Would there be an impact on employee morale if they found they were repairing counterfeit products?

**PRODUCTION DEPARTMENT**

**IF A DOCUMENT SECURITY OR COUNTERFEIT ATTACK OCCURRED, HOW WOULD THIS AFFECT PRODUCTION?**

Would production have to increase overtime to replace product in the market?
Do you have the capacity to manage the potential increase in production created by an attack?

Would you need to consider outsourcing to maintain volume?

What could be the potential costs of outsourcing to keep up with production requirements as a result of an attack?

What risks might be associated with outsourcing?

What production processes might need to be modified to protect against further attacks?

What additional employee training could be required to make modifications to the production process in response to an attack?

What are the potential costs of modifying production to protect against further attacks?

How would an attack impact the morale of production employees?

**PRODUCTION, SALES AND MARKETING DEPARTMENTS**

**WHAT ISSUES COULD ARISE IF A DOCUMENT SECURITY OR COUNTERFEIT ATTACK CAUSED AN INTERRUPTION IN PRODUCTION?**

What issues would arise if an attack caused a short-term shutdown of production?

What issues may arise if a counterfeit attack caused a long-term shutdown?

Could an interruption in production cause employee layoffs or short shifts?

Could you potentially lose employees due to an interruption in production?

Could you potentially lose customers due to an interruption in production?

How would an interruption in production affect customer perceptions of the company, its products and services?

How would an interruption in production affect employee morale?

**SALES AND MARKETING DEPARTMENTS**

**IF A COUNTERFEIT ATTACK OCCURS, HOW WOULD THIS AFFECT YOUR BRAND IMAGE?**

What marketing tactics would be required to rebuild your brand?

How long could it potentially take to rebuild your brand image?

What would be the projected costs of a long-term campaign designed to repair your company’s brand image?

How would the company alert customers of a document security or product counterfeit occurrence?
What is the potential cost of that notification process?

What would the necessity of an attack notification distributed to customers cost the company in terms of customer loyalty?

How would an attack impact the morale of the sales and marketing teams?

LEGAL DEPARTMENT

ONCE A DOCUMENT SECURITY OR COUNTERFEIT ATTACK OCCURS, WHAT LEGAL PROCESSES WOULD BE IMPLEMENTED?

What would be the anticipated time required to refute or settle any claims?

What dollar value is equated to that time?

What is the potential dollar loss attributed to paying settlements?

During the litigation timeline, is it possible that production could be interrupted or suspended?

What other legal processes and cost may arise due to a counterfeit attack?

EXECUTIVE MANAGEMENT

WHAT IMPACT WOULD A DOCUMENT SECURITY OR COUNTERFEIT ATTACK HAVE ON YOUR COMPANY OVERALL?

What is the value of an average customer to your company?

What is your hourly revenue per production hour?

What would it cost to replace a long-term customer in terms of sales force time and marketing cost?

Would an attack provide an opportunity for competitors to acquire some of your company’s market share?

What impact would an attack that caused an interruption or suspension of production have on the company’s brand and customer loyalty?

Could attacks lead to employee departures from the company due to a loss of confidence?

If one or more attacks occurred, what level of impact would occur to employee morale, and how would that affect the company?

How damaging would a document security or counterfeit attack be to the company overall?
DOCUMENT SECURITY:

Are Your Documents Safe?

Fraud is a massive problem and it affects nearly every business, creating tremendous losses for companies and individuals through a myriad of potential attack methods.

Any company or organization that issues documents of value or identity runs the risk of having those documents fraudulently altered or reproduced. Such fraud can have serious financial and legal implications for the issuing entities and for their customers. Potentials exist to cause severe damage to corporate reputations resulting in a loss of customer confidence in their brands.

THE RISKS

According to the Document Fraud Institute, “Each year, U.S. companies lose more than $600 billion to fraud, with ‘counterfeit and document fraud’ making up more than two-thirds of that.” (http://www.document-fraud.org/date/2010/12) Losses to businesses drive up costs, which in turn pushes up the price of products to the consumer. Since the 9/11 terrorist attacks, ID theft has accelerated and become a huge concern, since fake ID’s and related documents can be used to gain unauthorized access to critical areas and information. Fake identity can also allow criminals and illegal aliens access to government services and resources, putting a further drain on taxpayer funds.

The types of printed documents and materials that should contain security protections against fraud are more far reaching than many people may think, and it’s critical that companies secure their sensitive printed documents to protect themselves and their customers. Issuers of sensitive documents have a responsibility to show due diligence to deter fraud, especially if their documents contain personal identification information.

DEFENDING PRINTED DOCUMENTS AGAINST ATTACK

Document security features come in two primary types – covert (hidden) and overt (visible). By layering a combination of multiple features into any given document, increased levels of security protection are achieved. Layering begins with a substrate, or specialized paper, that may itself contain protective features such as watermarks, chemical sensitive stains, invisible fibers and so on. Other subtle or covert elements such as “void” pantographs produce visible warnings when a document is scanned or copied. The images printed on the documents themselves may incorporate specialized covert or overt security inks, foils, microprinting, encoding, etc., all designed to make the job of unauthorized reproduction as great a challenge as possible.

But there is no “silver bullet” of document security. Counterfeitters and thieves are always probing for weaknesses, and finding new ways to overcome various defense techniques. Layering document security elements is a best practice to offer a strong defense against attacks, offering significant challenges for potential attackers to overcome. It’s like putting “the club” onto the steering wheel of your car; your vehicle already has door locks, a keyed ignition and perhaps an alarm, but “the club” acts as a further visible deterrent to a potential thief, who will typically look for easier targets.

SOURCING SECURE DOCUMENT PRODUCTION

It’s critical to work with a print partner who has proven expertise and experience in the design, development and manufacturing of secure documents. The right print partner can walk a company through the process of risk analysis, including a thorough examination of past and current attacks that have occurred (i.e. mechanical, chemical or digital), as well as an assessment of potential future attack methodologies.

Then that print partner must have the extensive resources, equipment, and expertise necessary to design and manufacture appropriate solutions, all in a secured production environment. Companies who choose the right
print partner for their secure document design and production will gain a better understanding of their true level of risk, and have confidence they are doing everything possible to protect against potential liabilities.

**PEACE OF MIND**

While no document security methods are fool proof, companies who take a proactive approach to document security will realize a number of benefits. The costs of fighting fraud can be reduced and the loss of revenues due to fraud will be minimized. Potential liability and associated legal fees can decrease, document authentication will be faster and more accurate, consumer problems and complaints may go down, and the integrity of brand identities will be protected. Just as important, customers will recognize your expertise and your proactive interest in protecting their personal information and the value of the products they purchase from you.

**SUMMARY**

Access to technology has made it increasingly easy for amateur and professional counterfeiters to replicate and alter value documents. Combating these technologies requires a layering approach in substrate and print using both covert and overt solutions. This provides not only a means of counterfeit deterrent but also a means of document authentication which is often as critical as defending against the counterfeit activity itself.

Additional information sources:
www.dhs.gov
www.naspo.info