FRAUD FIGHTER™ by UVeritech

WHITEPAPER

COUNTERFEIT FRAUD PREVENTION
TIPS, TOOLS & TECHNIQUES

An Overview of Counterfeit Document Fraud & the Methods Available to Detect & Deter It

Sean Trundy,
COO

Table of Contents

Introduction 3

Counterfeit Fraud 4

Counterfeit Currency 4

Types of Counterfeit Dollars and How to Spot Them 8

Counterfeit Negotiable Instruments 10

Detecting Counterfeits 16

Visible Features 16

Latent Features 19

Scientific Analysis 22

Tools for Counterfeit Document Detection 24

Visible Review Aids 24

Advanced Analysis Devices 28

Currency Detection 28

Identity Document Detection 28

Multi-Layered Approach to Fraud Detection 30

Multiple Points of Vulnerability – A Case Study 31

Conclusions 32

Introduction

As financial transactions become more global and more virtual, the threat of financial crimes has increased as well. In fact, for more than a decade nearly all categories of fraud involving forgery have shown a consistent and disturbing upward trend year after year. As a result, worldwide financial losses resulting from counterfeiting are mounting, threatening not only individual and corporate profits but also jeopardizing international markets and governments. The threat is particularly acute in the realm of forged monetary instruments and identity documents. The evolution of sophisticated printers, computer software and other technological factors has increased the capacity of non-professional counterfeiters to create realistic fake documents and avoid detection by regulators and law enforcement. This, in turn, has spurred a cottage industry of outlaw organizations of counterfeiters - which in turn has flooded the market with forged documents for the purpose of defrauding the public.

Interactions with stakeholders – customer verification, document acceptance, payment processing etc. – common to virtually all organizations are becoming increasingly complex. Transaction-level employees are burdened with the nearly impossible task of authenticating thousands of transactions and recognizing possible forgeries. As a result, restaurants, banks, retailers and federal, state and local agencies are exposed to losses from this increasingly common form of fraud.

Criminal forgers aim to replicate a document that conveys some value or benefit to the person possessing it. Currency and identity records, of course, are common forgery media, but any document with intrinsic value can be counterfeited, from cash to checks to credit cards – even store coupons.

The ability to recognize, reject, and prevent forgery is of paramount importance to any organization. The potential for financial loss is obvious and businesses can quickly lose credibility – and customers – if their fraud-prevention measures prove inadequate. In addition, failure to property validate documents can result in legislative, regulatory and judicial punishment in the form of fees, penalties, civil litigation and even criminal prosecution.

This report strives to shed light on the current state of counterfeiting and discuss the methods and strategies available to public-facing organizations to recognize forged documents when they are presented.

Counterfeit Fraud

When most people think of counterfeiting, they typically conjure images of one of two scenes:

1. An ink-stained wretch with a magnifying glass in one hand and an engraver's tool in the other, as a printer spits out bogus banknotes in the background

2. A furtive "salesman" in a cheap suit peddling ersatz Rolexes and Gucci bags out of his car trunk.

But counterfeiting encompasses much more than just fake money and luxury products. The scope of this report encompasses the criminal production and presentation of documents in order to gain a benefit. As noted, the variety of documents susceptible to forgery extends well beyond currency:

- Negotiable instruments (cash, personal, cashier's and traveler's checks, money orders, gift certificates)

- Identification documents (passports, birth certificates, drivers licenses)

- Ownership documents (automobile titles, real estate deeds)

- Certificates of authenticity (antiques, rarities, collectibles, memorabilia)

- Store currency (coupons, promotional "dollars," loyalty points)

- Plastic (credit cards, debit cards, purchasing, procurement or P-cards)

Counterfeit Currency

Criminals have been making counterfeit coins and currency for as long as they have been making the real thing. In fact, counterfeiting is considered by many as the second-oldest profession. Law enforcement and legitimate businesses have been struggling to keep up ever since the first counterfeiter began using gold- and silver-clad base metals to replicate in 6th century B.C. Greece.

The United States redesigned its paper money in the 2000s and 2010s for two primary reasons, according to the Treasury Department: To "ensure that U.S. currency employs unique and technologically advanced features to deter counterfeiting," and to "facilitate the public's use and authentication." But America's battle against counterfeiters traces back to colonial times when unscrupulous settlers would dye white shells a deep indigo color to resemble the wampum so valued by Native Americans. During the 19th century counterfeiting became so rampant at times that shopkeepers refused to accept any paper money from the more than 1,500 banks authorized to print it. Even after the formation of the Federal Reserve Bank centralized American currency production, counterfeiting remained widespread. Following the Civil War, as much as one-third of U.S. money in circulation may have been counterfeit. The problem drove President Abraham

Lincoln to create the Secret Service, with the singular expressed mission of weeding out counterfeit money.

The Current State of Currency Counterfeiting

Technology

For much of history, counterfeiting paper currency required substantial investment and no small amount of skill. Early counterfeiters often hand-drew their notes. Even with the invention of the offset printer at the turn of the 20th century, counterfeiters' ability to produce high-quality photographic plates, reproduce real notes and mix ink colors were critical if they were to outflank government countermeasures.

Primary among these security advancements, the intaglio printing process uses heavy presses to force ink deep into the paper, creating the distinctive raised-texture recognizable to anyone who has ever handled a Federal Reserve note. Offset printing cannot generate the force necessary to perfectly recreate this feel; still, with care good forgers can create results good enough to pass.

The United States has adopted many additional security features in its legitimate currency, from intricate scrolling and image-shifting 3-D effects to green and black ink to special paper in an attempt to foil counterfeiters. Some features of money are especially hard to reproduce, such as the fine red and blue fibers that are embedded in the paper, or specialty ultra-violet or infra-red inks that are difficult to work with. While these measure typically present challenges for all but the most determined counterfeiter, many can simply omit these features altogether and still manufacture forgeries that pass visual inspection. The Fraud-Fighter™ line of ultra-violet counterfeit scanners, however quickly and efficiently detects these types of fakes.

Traditionally, after producing an acceptable copy, the counterfeiter would print large quantities of the forged note, in an effort to reap a reward from his illegal activities. This would necessitate the difficult task of circulating the bills, usually leaving a literal paper trail both forward to his partners in crime who received the counterfeits in bulk, and backward to the suppliers of the special inks and paper. The difficulty of hiding such large-scale conspiracies regularly led to their discovery by law enforcement, whose historical success in seizing fake money prior to its circulation has been exemplary.

Today, sophisticated computers, high-resolution reprographic software and photo-quality printers have reduced the initial investment and reliance on human artistic ability. With an investment of less than $1,000, nearly anyone can become a clandestine counterfeiter, printing notes in his or her basement or spare bedroom that can easily fool a department store cashier. Fake notes made digitally on an inkjet printer, though of noticeably lower quality than those produced on an offset press, frees the forger from the need to involve others in the production and distribution process. The counterfeiter can print a handful of $20 or $100 bills whenever they are needed, rather than creating large batches for laundering. From 1995 to 2015, the confiscated notes produced digitally grew from 1 percent to more than 60 percent. Not surprisingly, the Secret Service, faced with much smaller, more dispersed operations, has seen its domestic seizure rate fall steadily from 70 percent in 1995 to about 10 percent in 2016. The result has been a dramatic increase in the number of counterfeit bills reaching the public.

Organized Crime Involvement

While the relatively low initial investment required to begin counterfeiting currency digitally has led to a spike in the number of operations tied to street gangs and the drug trade, foreign organized crime organizations, continue to exploit both offset printing, wide distribution networks and plentiful artisans to produce high-quality fake bills in large quantities.

Professional counterfeiting factories operated by international mafia groups use efficient production and quality control processes such as TQM and Six Sigma to create consistently high-quality fakes, and are able to learn and improve from each iteration of the production run.

The sheer scale of these “forgery factories” is staggering:

- Just one year after police seized $3.7 million in counterfeit U.S. currency in a 2013 raid in Thailand, authorities intercepted $7.2 million at the Thai/Cambodian border.

- In 2009, Wilson Liu, a Taiwanese national responsible for bringing as much as $25 million in “supernotes” into the U.S. gave evidence to the FBI in which he implicated Chinese and Russian Mafia families in the dissemination of the high-quality fake $50 and $100 bills produced by North Korea.

- In November 2016, Peruvian authorities and the Secret Service made the largest haul of forged bills in history - $30 million during a series of raids around Lima. The operation resulted in the arrest of 48 people and the closing of six printing plants.

Foreign counterfeits account for over 80 percent of all offset counterfeit notes and about 60 percent of the total volume of counterfeit U.S. currency produced in the 21st century. With nearly 75 percent of the total legitimate U.S. currency supply held overseas, and with the $100 bill far more common abroad than it is in the United State, it is not surprising that the most commonly counterfeited bill outside the United States is the $100 (domestically it is the $20).

Foreign Government Involvement

Counterfeiting an enemy’s currency to destabilize the government is a time-honored wartime tactic. American and British intelligence operations attempted it during the Revolutionary War. Britain tried to counterfeit German marks during World War I. And the Nazis carried out an extensive operation to flood the United Kingdom with forged Bank of England notes.

Today, rogue states such as North Korea, Syria and Iran invest in expensive intaglio presses quite similar to those used by the Bureau of Engraving and Printing to print forged U.S. legal tender. Rather than using the supernotes they produce as weapons for destabilizing the American economy, these countries most often use the counterfeit funds in an attempt to prop up their own economies. The Secret Service acknowledges that the uneven regulatory procedures, banking practices and law enforcement activities abroad may result in radical underreporting of the amount of U.S. currency changing hands overseas. Still, the "pass rate" for counterfeit U.S. currency abroad is extremely low, as a result of its detection and seizure in large quantities before it goes into circulation.

Currency Counterfeiting on the Rise

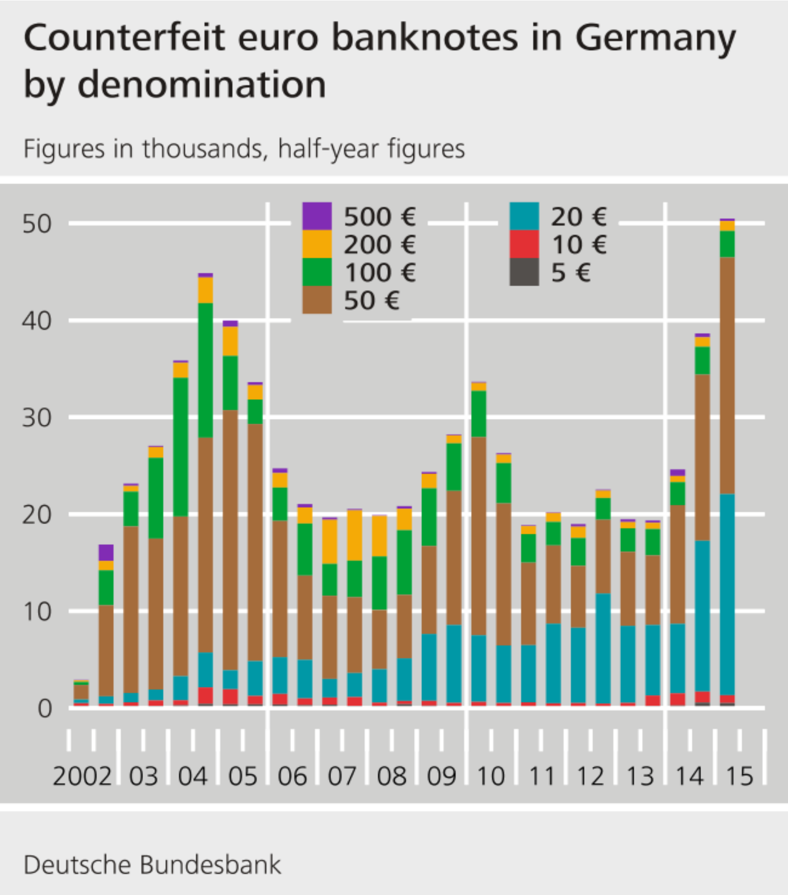
While only about 1 in 10,000 Federal Reserve notes are bogus, the quantity and purported value of counterfeit U.S. bills in circulation continues to rise. The amount of forged money passed and later discovered has grown apace as well. The progression mirrors the evolution of low-cost, high-quality imaging and printing technology. Before this equipment became readily available, "passed" counterfeit currency remained relatively steady –$39.2 million in 1999, $48 million in 2001 and $42 million in 2006. But the numbers skyrocketed 63 percent to $62 million in 2006 and another 66 percent to $103 million in 2013. The trend continues, with $156 million – more than half collected in the United States – identified in 2015. As technology has made it easier to produce viable counterfeit banknotes, the number of such counterfeits circulating has increased.

Anecdotally, we can validate this information through the conversations our company has with our U.S. customers on a daily basis. Retail businesses – whether involved in merchandizing, food service, hospitality or financial services – report that the losses experienced at the store level due to counterfeit currency are increasing at exponential rates. In fact, it is our belief that the officially quoted numbers are under-reported, and that circulating counterfeit currency numbers are much higher than those provided by the Secret Service and the General Accounting Office.

North Korean Superdollars

The United States has accused the Democratic People's Republic of Korea (DPRK or North Korea) of counterfeiting U.S. $100 Federal Reserve notes (Supernotes) and passing them off in various countries, although there is some doubt by observers and other governments that the DPRK is capable of creating Supernotes of the quality found. What has been confirmed is that the DPRK has passed off such bills in various countries and that the counterfeit bills circulate both within North Korea and around its border with China. Defectors from North Korea also have provided information on Pyongyang's counterfeiting operation, although those statements have not been corroborated. Whether the DPRK is responsible for the actual production or not, trafficking in counterfeit has been one of several illicit activities by North Korea apparently done to generate foreign exchange that is used to purchase imports or finance government activities abroad.

Nanto, Dick K. North Korean Counterfeiting of U.S. Currency. June 12, 2009



Counterfeit euro banknotes in Germany by denomination

Figures in thousands, half-year figures

Deutsche Bundesbank

The counterfeiting issue is not confined to U.S. dollars. Currencies around the globe are under attack. The chart to the left shows counterfeiting numbers involving the Euro, from the year of the release of the Euro in 2002, through 2015. The individual data points are tallied in 6-month intervals. What can be seen here, obviously, is the instant appearance of counterfeited Euro notes after it was first released, then a leveling-off period from roughly 2004 thru 2007, followed by two years of data in which sharply increasing volumes of counterfeits are seen. This trend can be tracked for numerous other world currencies, as well – the Japanese Yen, British Pound and Swiss Franc all are seeing the same reaction to the conditions outlined in the previous section, namely, the ease of access to digital counterfeiting tools, and the involvement of both organized crime and government-backed currency terrorism. Most important is the third spike beginning in 2014 and continuing today.

German law enforcement and banking officials believe the rising incidence of counterfeit Euros in recent years is owing to even greater consolidation and professionalization of the illegal enterprise among organized crime, outlaw nations, and terrorist groups who produce large quantities and either use it for their own purchases or sell it on the internet. The digital underworld also provides a marketplace for counterfeiting supplies and the exchange of best practices and trade secrets, adding to the prevalence of forged banknotes in Europe and Asia.

Types of Counterfeit Dollars and How to Spot Them

Digital Notes

The most ubiquitous type of counterfeit notes circulated in the United States are created using common office equipment – digital scanners, desktop computers, graphics software and color inkjet printers. In their simplest form these “digital notes” are copies of genuine bills. The forger scans or photocopies a real $20, $50 or $100 bill, enhances the image in a graphics program and prints it on a high-resolution inkjet or laser jet. Technology has made these counterfeits virtually indistinguishable from real currency by the naked eye. Printer jets are capable of delivering a single, tiny droplet of ink to a precise location on a page; image acquisition software can capture the ultrafine details on a banknote, including microprinting and security threads; Over-the-counter printers can blend toner and ink to very closely replicate the colors produced on US banknotes, essentially undoing one of the oldest defenses that the US currency has against counterfeiting – the unique green and black ink colors used in their production.

Law enforcement continues to make strides against digital forgers. Many copy machines, for instance, how come equipped with software that can recognize when a U.S. banknote has been placed on the machine. The software is designed to shut down the copier to prevent copies being made and in some cases to even notify law enforcement that someone has attempted to photocopy a bill.

Still, technology continues to make great leaps forward; quality improves and prices drop, making counterfeiting a tempting part-time "job" for some. The Secret Service reports that nearly 70 percent of the $78 million in counterfeit U.S. notes passed on American soil in 2015 was digitally produced, up from less than 60 percent in 2013.

Washed Notes

Bona fide U.S. paper money is printed on paper comprised of 75 percent cotton and 25 percent linen, producing "feel" and ink absorption qualities counterfeiters find difficult to replicate. In addition, the widespread adoption by businesses of the "counterfeit ink pen" made detection of counterfeit notes printed on incorrect paper an easy and low cost solution. Some forgers have found it expedient to "wash" banknotes for use in their digital forgery schemes.

In essence, a washed note is any counterfeit that uses a genuine lower -banknote as the "paper stock" upon which the higher-denomination counterfeit is printed. Counterfeiters use bleach, degreaser or other solvent solutions to remove the ink from a $1 or $5 bill. They then print a digital image of the $50 or $100 bill onto the now-blank bill using the digital method outlined above. The resulting counterfeit note can be very difficult for most people to detect. It feels real because the paper is real banknote paper, and the counterfeit ink pen will indicate a genuine banknote, because it is also simply testing the paper. If the counterfeiter uses a $5 bill as the base-stock, the bogus note will even feature both a security thread and a watermark. While these will not be the correct thread or the correct watermark for the "new" denomination, few store clerks bother to check for them, and many who do simply note that they are present, not whether they are genuine.

In 2014 Tarshema Brice pleaded guilty to printing between $10,000 and $20,000 in counterfeit cash. She soaked $5 in Purple Power degreaser, then scrubbed off the ink with a toothbrush before printing fake $100s and $50s onto the paper. Hardly a master printer, the 34-year-old hairdresser nevertheless passed the forged notes for two years before she was caught.

Supernotes

No one really knows who prints supernotes, also known as superbills and superdollars, which are virtually indistinguishable from legitimate currency, The U.S. government is convinced that these nearly flawless reproductions of pre-2013 $100 bills are the handiwork an adversarial foreign government (North Korea is a leading suspect) working with or without well-coordinated and well-funded criminal organizations. Supernotes, which began appearing in the late 1980s, are so realistic because they are created using the same or similar intaglio process the Bureau of Engraving and Printing uses to produce real bills. Because their equipment is so similar to the

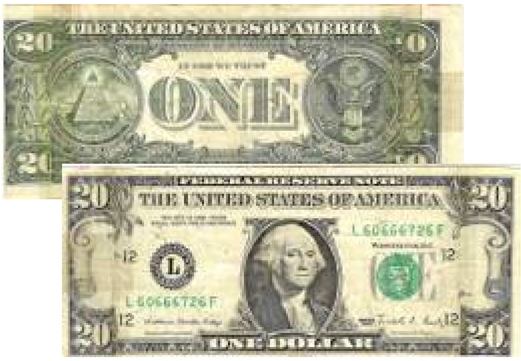
Bureau’s presses, they can replicate many of the security features in the greenback’s ink and paper.

The Secret Service believes North Korea has produced some $40 million in supernotes. While some observers have questioned whether the Pyongyang regime possessed the advanced technology and skill to print the high-quality forgery, it is known that the bills circulated freely in North Korea, especially near the Chinese border. Other suspects include Syria, Iran, Russia, and China. At least one journalist suggested the Central Intelligence Agency was involved, printing supernotes to fund clandestine operations overseas.

Supernotes began to disappear from circulation well before the U.S. introduced the new $100 bill with the large portrait of Benjamin Franklin, color-shifting Liberty Bell image and other features that make it nearly unforgeable.

Altered Bills

If supernotes represent the ultimate sophistication in the counterfeiters’ art, altered bills show the most rudimentary and unrefined forgery attempts. As the name suggests, altered notes are genuine banknotes that have been altered to change their appearance. Of course, this is done to increase the banknote’s denomination or face value. The common method for doing this has been to cut the four different numeric-corners off four different high-denomination banknotes, and glue them onto a $1 bill. Examples are seen in these images to the right, where the corners clearly show the $20 value, while the rest of the bill displays the $1 dollar features, including clearly-printed text on both front and back reading “one,” and .



This type of counterfeit really is outdated and is not likely to be seen very often these days. There was a time, however, when this was a common technique for passing counterfeit notes. The forger would make payment at a retail establishment with a stack of bills in which the altered note was inserted. The poor cashier, conducting a quick-count of the money, would look only at the corners as he/she tallied the payment. Often, the counterfeit wouldn’t be noticed until the bank caught it while processing their deposit.

The clever part of the altered note is that it can pass a number of cursory tests that might be conducted at the cash register, such as the “feel” test (it is, after all, a real banknote) and the counterfeit ink pen test (for the same reason – it is real banknote paper). As long as the acceptor doesn’t pay close attention to the full detail of the bill, it is possible for a busy cashier or a cashier in a dimly lit environment such as a bar or nightclub to accept this type of counterfeit bill without being aware of it.

Counterfeit Negotiable Instruments

Currency is not the only type of document that is regularly forged. As previously discussed, almost any type of document which conveys to its holder some value may become a target for counterfeiting. The multitude of different types of document designed to deliver monetary value creates a long list of possible counterfeit fraud items.

Money Orders

Most people think of money orders safe, virtually the equivalent of cash. Since it isn’t a personal check, there is no danger of the money not being available when it is deposited. Unfortunately, it may not occur to the recipient that the money order may be a fake.

Perhaps the most widely publicized use of counterfeit Money Orders and Postal Money orders has been via the “Nigerian” or “advanced fee” scam and its variations. Under these types of scams the con-artist tricks the victim into depositing a counterfeit money order and sending a part of the proceeds back to the fraudster via a gift card or wire transfer. Whether the returned funds are presented as finders’ fees, accidental overpayment, taxes on monetary prize won or some other detail, the scam works because only after the cheat redeems the returned portion is the victim notified that the money order was no good and that he or she is liable for the funds obtained from the bogus document.

REPORTED COUNTERFEIT CASHIER’S CHECKS

6/9/2016 - Provident Savings Bank, FSB Riverside, CA

3/30/2016 – Washington Federal Bank, Seattle, WA

3/15/2016 - Pioneer Bank, Roswell, NM

2/24/2016 – First National Bank & Trust, Iron Mountain, MI

1/28/2016 – Valley National Bank, Wayne, NJ

12/24/2016 – Carrollton Federal Bank, Carrollton, KY

12/24/2016 – First National Bank, Davenport, IA

12/2/2016 – Banc of California, Irvine, CA

10/9/2015 – First Federal Bank of Ohio, Galion, OH

9/30/2015 – LCNB National Bank, Lebanon, OH

9/24/2015 – First Financial Bank, Hamilton, OH

8/23/2015 – Northfield Bank, Woodbridge, NJ

8/23/2015 – First Federal Bank, Dickson, TN

8/23/2015 – First National Bank of Bastrop, Bastrop, TX

6/29/2015 – Citizens Savings Bank, Clarks Summit, PA

6/28/2015 – CenterState Bank of Florida, Winter Haven, FL

6/16/2015 – BFSFCU Bank-Fund Staff Federal Credit Union, Washington, DC

6/15/2015 – Arrowhead Credit Union, Winchester, VA

What makes this type of fraud-loss most unfortunate is that genuine money orders are, typically, fairly well-secured documents. That means that – if one knows what to look for – authentication is not very difficult. As added protections, call the issuing bank, retail outlet, or agency, cash the money order at the same location it was supposedly purchased. Unfortunately, with so many documents in circulation, the chance that any given person will know what to look for is small.

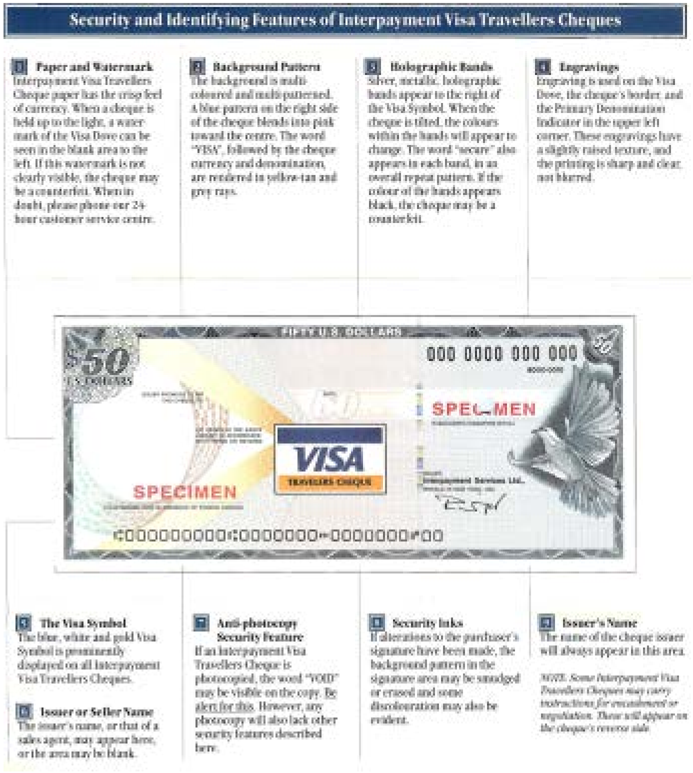
Cashier’s Checks (Official Checks)

Cashier’s checks, like money orders, are typically considered to be risk-free, as the funds backing the check are drawn directly against a bank and not against an individual’s checking account. This fallacy puts potential victims of counterfeit cashier’s checks at risk, lulling them into a false sense of security and leading them to forgo the typical “common sense” practices they otherwise would employ when receiving a payment from a stranger.

Cashier’s checks are no less likely to be forged than personal checks. In some respects, they may even be MORE likely to be forged precisely because they don’t receive the same scrutiny a personal check might. The inset box on the right side of this page shows a recent one-year period during which 18 different U.S. banks reported that their cashier's checks had been counterfeited. As can be seen from this small sample, counterfeiting strikes banks and credit unions of all sizes, and from all corners of the country.

Traveler's Checks

Despite the fact that traveler's checks are typically designed to be quite secure, counterfeits continue to plague the market. In this scam, fraudsters typically purchase traveler's checks in small amounts, then alter those amounts to reflect larger denominations. The con artists then either make small purchases, pocketing the change in cash or make large purchases, either keeping the big-ticket items or returning them for case refunds.



Security and Identifying Features of Interpayment Visa Travellers Cheques

1 **Paper and Watermark**
Interpayment Visa Travellers Cheque paper has the crisp feel of currency. When a cheque is held up to the light, a watermark of the Visa Dove can be seen in the blank area to the left. If this watermark is not clearly visible, the cheque may be a counterfeit. When in doubt, please phone our 24-hour customer service centre.

2 **Background Pattern**
The background is multi-coloured and multi-patterned. A blue pattern on the right side of the cheque blends into pink toward the centre. The word "VISA", followed by the cheque currency and denomination, are rendered in yellow-tan and grey rays.

3 **Holographic Bands**
Silver, metallic, holographic bands appear to the right of the Visa Symbol. When the cheque is tilted, the colours within the bands will appear to change. The word "secure" also appears in each band, in an overall repeat pattern. If the colour of the bands appears black, the cheque may be a counterfeit.

4 **Engravings**
Engraving is used on the Visa Dove, the cheque's border, and the Primary Denomination Indicator in the upper left corner. These engravings have a slightly raised texture, and the printing is sharp and clear, not blurred.

5 **The Visa Symbol**
The blue, white and gold Visa Symbol is prominently displayed on all Interpayment Visa Travellers Cheques.

6 **Issuer or Seller Name**
The issuer's name, or that of a sales agent, may appear here, or the area may be blank.

7 **Anti-photocopy Security Feature**
If an Interpayment Visa Travellers Cheque is photocopied, the word "VOID" may be visible on the copy. Be alert for this. However, any photocopy will also lack other security features described here.

8 **Security Inks**
If alterations to the purchaser's signature have been made, the background pattern in the signature area may be smudged or erased and some discolouration may also be evident.

9 **Issuer's Name**
The name of the cheque issuer will always appear in this area.

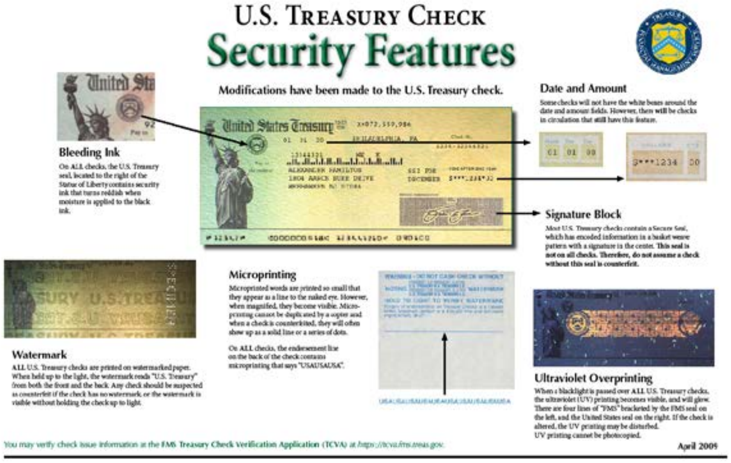
NOTE: Some Interpayment Visa Travellers Cheques may carry instructions for encashment or negotiation. These will appear on the cheque's reverse side.

It is difficult to find statistics regarding this issue, but we have voluminous anecdotal evidence to suggest that it is a leading cause of cash register shrink at retail, quick service restaurant, convenience and banking establishments. UVeritech surveyed a cross section of more than 300 respondent customers and found that 79 percent of them had accepted counterfeit traveler's checks in the previous 12 months.

Visa distributed the circular to the left to educate cashiers on the numerous physical (e.g. "overt") security elements contained within traveler check designs. However, with numerous major companies (Visa, MasterCard, American Express, Diners Club and Thomas Cook, etc.) along with smaller banks and credit unions issuing such checks and each company issuing several different designs, often for several different currencies, knowing and understanding how to validate the authenticity of such checks is a serious issue. Cashiers cannot reasonably be expected to remember all these details.

Treasury Checks

Every year, the federal government collects more than 70,000 forged or altered U.S. Treasury checks accounting for losses approaching $100 million annually. These numbers conform to a long-term trend dating back at least 65 years. In 1941, the U.S. Congress authorized the establishment of the Check Forgery Insurance Fund to serve as a restitution source to payees when checks drawn upon federal treasury



U.S. TREASURY CHECK
Security Features

Modifications have been made to the U.S. Treasury check.

Bleeding Ink
On ALL checks, the U.S. Treasury seal, located to the right of the Statue of Liberty contains security ink that turns reddish when moisture is applied to the black ink.

Date and Amount
Some checks will not have the white boxes around the date and amount fields. However, there will be checks in circulation that still have this feature.

Signature Block
Most U.S. Treasury checks contain a Secure Seal, which has encoded information in a basket weave pattern with a signature in the center. This seal is not on all checks. Therefore, do not assume a check without this seal is counterfeit.

Watermark
ALL U.S. Treasury checks are printed on watermarked paper. When held up to the light, the watermark reads "U.S. Treasury" from both the front and the back. Any check should be suspected as counterfeit if the check has no watermark, or the watermark is visible without holding the check up to light.

Microprinting
Microprinted words are printed so small that they appear as a line to the naked eye. However, when magnified, they become visible. Microprinting cannot be duplicated by a copier and when a check is counterfeited, they will often show up as a solid line or a series of dots.

On ALL checks, the endorsement line on the back of the check contains microprinting that says "USAUSAUSA".

Ultraviolet Overprinting
When a blacklight is passed over ALL U.S. Treasury checks, the ultraviolet (UV) printing becomes visible, and will glow. There are four lines of "FMS" bracketed by the FMS seal on the left, and the United States seal on the right. If the check is altered, the UV printing may be disturbed.
UV printing cannot be photocopied.

You may verify check issue information at the FMS Treasury Check Verification Application (TCVA) at https://tcva.fms.treas.gov.

April 2009

depositories had been lost, forged or stolen. This fund still exists today.

Personal Checks

Personal checks are a forger's playground.

Check fraud and identity theft continue to be the fastest growing financial crimes in America. Even as online banking and retailing continue to grow, claiming an ever-increasing share of financial transactions, losses from forged checks topped $13 billion in 2015. This, even as the number of checks being written has fallen from about 36 billion in 2003 to 13 billion in 2015. Losses per bad check have doubled over that timeframe as well. To put those statistics in perspective, every single check written and cashed, whether by a bank, store, utility, landlord or other entity, there is a $1 fraud loss "built in" to that check. .

According to Association for Finance Professionals statistics for 2012, 66 percent of businesses responding to a survey were victimized by counterfeit personal checks presented as payment.

Check fraud gangs continue to be innovative and industrious. They constantly try new concepts and techniques to beat the banking system and steal money. Historically, the banks have been liable for these losses. However, recent changes in the Uniform Commercial Code now assign shared liability between the bank and the depositor in most instances.

The American Bankers Association's Deposit Account Fraud Survey, which collects baseline information on check and electronic payment fraud losses, estimated that industry check-related losses amounted to $1.91 billion in 2015, up slightly from the $1.744 billion in 2014.

Check fraud experts – on both sides of the law – have outlined the dangers of conducting business by check.

Frank Abagnale, the infamous check forger who inspired the film *Catch Me If You Can*, noted,

> "On that check is my name, address, phone number, my bank's name and address, my bank account number, routing number, and my signature."

A store clerk would typically also write on the check the account holder's driver license number, date of birth and sometimes, his Social Security number.

No one can be completely confident that store employees will guard the information they collect, Abagnale said.

> "What I do know is that anyone who sees the front of that check has more than enough information to draft on my bank account."

Store Coupons and Store Currency

Coupon fraud – the illegal reproduction of commercially issued discount coupons or store promotion currency – costs manufacturers and retailers more than $500 million annually. Considering about $5 billion worth of coupons are redeemed each year, 10 percent of the money saved through coupon use is collected illegally.

Scam artists often copy legitimate coupons and change expiration dates, product names or the amount of the discount. Sometimes coupons that are printed in circulars are scanned or photocopied. The fake coupons are then distributed through e-mail, Internet discussion groups and online auction sites. Some counterfeiters sell or trade them. Most counterfeit coupons cover a wide variety of brands and involve mostly "free" product offers.

Coupon fraud is such an epidemic that in 2013 eBay banned or severely limited the sale of coupons on its platform. "So the counterfeit coupon market began migrating underground," the *Coupons in the News* website reported in 2015. "Today, if you know where to look, you can find loads of counterfeit coupons available for sale online, many of them in secret and closed Facebook groups." The website reported the arrest of a North Carolina couple in possession of "874 counterfeit "free item" coupons…with a combined face value of more than $8,400. Responding to a survey, one consumer product manufacturer estimates its losses to counterfeit coupons at more than $3 million a year.

A similar scam entails the alteration or forgery of cash register receipts to defraud stores. This return receipt scam can take many forms, including the purchase of items on sale, changing the price paid displayed on the receipt and then returning the item for the higher price. Perhaps more common, shoplifters steal merchandise and brazenly return it to the store for refunds, producing counterfeit receipts – often printed on cash register tape they also have stolen from the store. Return receipt fraud is now one of the leading causes of fraud loss in the retail industry, costing $9.1 billion according to a 2016 report by the National Retail Federation.

Any of these instruments may, at some point during the course of normal business in the United States, require a cashier to analyze and process as a form of payment. Unlike currency, which people understand is a counterfeit target and scrutinize accordingly, checks and other financial instruments purportedly issued by governments or banks are often considered "safe". Traveler's checks, money orders and other secured checks are backed by the underwriting institution, so the receiving party does not run the risk that the account may contain insufficient funds to cover the obligation. Similarly, people tend to not worry that the state or federal government will bounce a check and may be less cautious than prudence dictates.

Credit Cards, Gift Cards and Stored Value Cards **–** It is no surprise that credit card fraud has reached critical proportions. According to *The Nilson Report*, the cost of credit card fraud reached $16.3 billion worldwide in 2014 – more than 5 ½ cents per $100 in credit card transactions. The problem is ever worse in the United States, which accounted for nearly half the credit card fraud losses on less than a quarter of the volume.

The manner in which fraud on a credit card account can be conducted is quite varied. Ranging from outright theft of a valid card, to electronically "capturing" the card data and creating a forged copy of it, to using stolen identity information to fraudulently apply for a card in another person's name. Crooks can collect the data they need to perform credit card fraud in a number of ways:

- **Card not present (CNP) Transactions –** The mail and the Internet are major routes for fraud against merchants who sell and ship products, and these illegal activities affect legitimate mail-order and Internet merchants. If the card is not physically present when a purchase is made, the merchant must rely on the owner to supply the information indirectly, whether by mail, telephone or over the Internet. While there are safeguards, accepting credit card information over the telephone or on an online form is still more risky than recording it directly from a card shown in person at the point of purchase. Card issuers tend to charge a greater transaction rate for CNP to account and compensate themselves for the greater risk that the person presenting the card information is not the rightful owner. Shipping companies can guarantee delivery to a location, but they are not required to check identification. Moreover, they are usually not involved in processing payments for the merchandise.

- **Application Fraud –** Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Or they may create counterfeit documents.

- **Account takeover –** Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the legitimate cardholder to ask for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent to the new (bogus) address.

- **Skimming –** Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" perpetrated by a dishonest clerk, cashier, server or other employee. The thief can procure a victim's credit card number using methods ranging from simply photocopying receipts to more advanced techniques such as using a small electronic device (skimmer) to swipe and store hundreds of victims' credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of victims' credit card out of their immediate view. Thieves may also use small keypads to unobtrusively copy the 3 or 4 digit card security codes which are not present on the magnetic strip. Some ingenious skimmers have even placed devices over the card slots on ATMs. The skimmers read the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera focused on the ATM keypad to read the user's PIN at the same time.

- **Carding –** Once criminals steal a credit card, obtain account details or guess at a legitimate card number, they often make small online transactions to verify it is still valid and the account is still open. In this "carding" process, thieves present the card information on a website that has real-time transaction processing. If the card processes successfully, the crook knows that the card is still good; they typically will then sell the data files to other individuals who will carry out the actual fraud. The specific item purchased in the carding test run is immaterial, and the thief does not need to purchase an actual product; a website subscription or charitable donation is sufficient. The purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the card issuer's attention.

- **BIN Attack –** Because credit cards are produced in BIN ranges (the first 12 digits on the card), where an issuer does not use random generation of the card number, it is possible for attackers to obtain one good card number and generate valid card numbers by using the same BIN and changing only the last four numbers using a generator. The expiry date of these cards would most likely be the same as the good card.

As we have demonstrated, the losses incurred by businesses and individuals owing to the counterfeiting are alarming. And while the redesign of U.S. banknote has helped the Secret Service clamp down on forged currency, other forms of fraud – checks, coupons, and personal identification – continue to grow and play an ever-increasing role in not only theft, but also human trafficking, drug smuggling, terrorism and other heinous crimes.

Even worse, the economic impact of counterfeiting exerts additional costs due to a multiplier effect estimated at 3.1. That is, every dollar that is stolen via counterfeiting or document fraud, victims suffer $3.10 in losses in overdraft fees, returned check costs, penalties and lost productivity as they cancel credit cards, file police reports, insurance claims and more.

Detecting Counterfeits

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

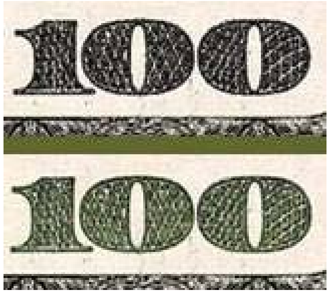
This, obviously, poses problems. Cashiers and tellers are often pressed for time as long lines of impatient customers demand they conduct transactions as quickly as possible. Add to this the vast array of different document types that must be verified, and the quantity of designs and styles that may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

Visible Features

When conducting visible document inspection, the acceptor is attempting to verify the presence of certain visible, or “overt,” security features:

- **Color-Shifting Ink –** U.S. currency has used shifting ink as a security feature since 2006. With the advent of the “big head” design, which began with the new $100 bill in that year, color shifting ink features have been added to the design of each lower denomination bills as they were introduced.

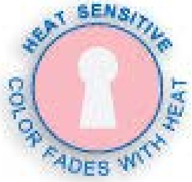
  Visual confirmation of this feature is quite simple. Look at the lower-right hand corner of the face of the bill, and notice the printed denomination numeral. Tilt the bill back and forth, thus changing the angle at which you view the number, and the color of the ink will "shift" from gray to green and back again. Color shifting ink is an effective, simple test that can be performed easily by a cashier. As long as lighting conditions are sufficient, this should be a valid technique to teach cash-handling employees. However, it should be noted that this feature can and has been defeated by enterprising counterfeiters, who have managed to replicate the general effect – in some cases quite well, and on other cases, with limited results.



- **Holographic Images -** Holography is an advanced-printing technique that creates the illusion of 3 dimensions on a flat, 2-dimensional surface. Pictured below is an example of a hologram. As the viewer turns and tilts the image, some colors appear to change, shadows and highlights emerge and the image gains "depth," with some elements appearing in the foreground and others receding. Holograms are commonly used as security features on traveler checks, credit cards and identity documents because theoretically they are difficult to reproduce and the holographic effect is visible to the naked eye. Unfortunately, the criminal element has created a black market where excellent facsimiles of the holograms used by major brand names (e.g. Visa, MasterCard, American Express, Cook's, etc.) can be purchased. Also, we have seen simple photocopies of holograms printed on metallic paper which can pass the cursory visual review often performed by cashiers in a hurry.

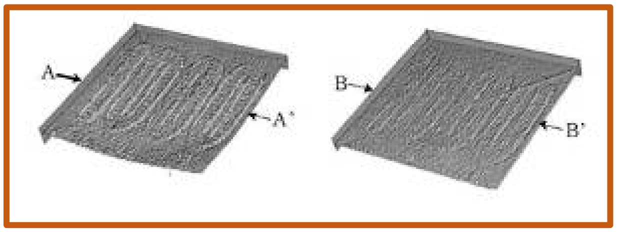
  Holograms affixed to passports and other identity documents typically come in many varieties and in greater detail, making them a better security measure for such documents, PROVI.D.ED THAT the person accepting the I.D. knows what to look for. UVeritech monitors websites that offer fake I.D. containing elaborate holographic images. If the teller or cashier receiving such a document has not been properly trained as to how the hologram should appear, these fakes can easily fool even the most attentive employee.

- **Thermal Ink –**Thermal ink changes appearance when it is heated. In the example pictured to the right, the acceptor places his or her thumb on the keyhole image, heating the ink and causing the red coloring to disappear. Once the paper cools again, the red ink will reappear. We have seen this type of security feature most commonly used on cashier's checks and money orders. We consider this to be a secure form of covert feature, since the technology to reproduce such features – while not advanced or difficult to emulate – requires specific chemistry and printing techniques typically beyond the counterfeiter's scope. Most counterfeit cashier's checks based on a template that uses thermal ink will include the

security image, but it will not be printed with thermal ink and will not actually change under different temperature conditions.

- **Intaglio Printing –** Intaglio is really the master overt defense for printed document security. Intaglio printing uses intricately carved plates and extremely heavy presses to physically alter the surface of the paper that is printed on. Very fine-details in the plates helps forced ink into the paper's fibers, creating a distinctive "raised feel" to the paper. The image viewed to the left shows an extreme magnification of a genuine intaglio-printed number "1000" (on the left) and an inkjet-printed "1000" (on the right). The genuine intaglio document shows just how clearly the ridges and edges of the numerals have been created. This is the result of the printing plates forcing the ink into the paper and causing the patterns to achieve a 3-dimensional texture. The inkjet cannot approach this effect. Intaglio printers can produce very fine detail.

  Consider the image of the U.S. $100 bill on the right. The very fine line details both on Benjamin Franklin's face and in the surrounding oval are produced at a level of resolution that inkjets and laser jets are unable to match. Also, running a thumbnail along the fine lines allows the cash-handling employee to feel the ridges produced by force the heavy press imparts to the paper. Because it is so difficult to reproduce both the resolution and the physical characteristics of intaglio printing, we believe that it is the best and most reliable of the "overt" features that can be used to verify documents.

- **Watermarks –** Watermarks come in two general categories "genuine" or "artificial." Contrary to what these terms may mean in the context of a discussion of counterfeit documents, both these types of watermark are "real." The difference between a genuine and artificial watermark is how the watermark is created. In the case of a genuine watermark, a pattern or image is carved into a mold which is used to "emboss" the image into the paper. The watermark is physically stamped in a technique that produces both a visible image and a below-the-surface raised depiction of the image. Artificial watermarks, on the other hand, are really replicas or facsimiles of genuine watermarks. This type of watermark is printed on the surface of the paper, but the printing is designed so that it is not easily

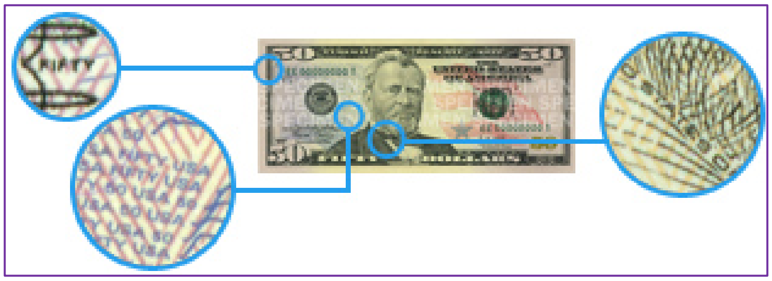
  ORIGINAL
  DOCUMENT

visible unless viewed from an angle, or with a backlight. Watermarks are commonly used in currency notes, traveler's checks, many types of cashier's checks, money orders, gift checks and more. As a security feature, they are not very effective. Counterfeiters have found many ways to create realistic watermark facsimiles. In fact, many common word processing and graphics programs allow users to add artificial watermarks with the click of a mouse. When printed with special, yet readily available inks, the overall effect of the counterfeit watermarks can be nearly indistinguishable from the real thing.

Latent Features

Latent, "covert," features are, by definition, designed specifically to be invisible to the human eye under normal conditions. Tools or devices must be used to verify the presence of such features. There are a number of different techniques to covert features:

- **Microprinting –** As the name suggests, microprint is a technique in which extremely small, finely detailed printing is included on a document. In the case of U.S. currency notes, microprint features are typically words printed in characters too small for the naked eye to see. As the example to the right shows, microprint security features in several locations on the newest U.S. $50 banknote design. Many of the world's major currency notes contain microprint security features.



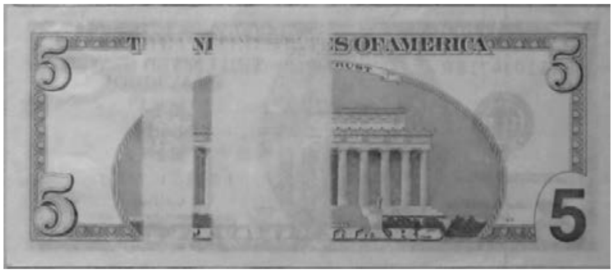
This second image is a sample of the $10 Australian banknote, which includes a microprint poem.

In addition to currency, microprint is commonly used to secure money orders, cashier's checks and many different forms of identity documents. Because the high resolution required for microprinting can be achieved only with offset presses, we assess this security measure to be relatively effective. This is beyond the capabilities of a very high percentage of counterfeiters who are "digital artists" and do not possess the skills or the equipment to perform offset printing. However, from a retail/operational perspective, undertaking a microprinting validation during a transaction is both intrusive and time consuming. The teller or cashier must use a magnifying glass or magnification imaging device to properly see the microprint. This is a rigorous process. Meanwhile, the customer sees his I.D. or payment being scrutinized with a magnifying glass, and the "customer experience" – an important consideration for many businesses – is jeopardized.

- **Infrared Printing –** Infrared inks are invisible because the wavelengths they reflect are longer than those the human eye can perceive. To detect IR features in documents, the paper must be exposed to a device capable of rendering the IR inks into the human-visible spectrum. This is typically achieved with an imaging-scanner equipped with an infrared lens. The lens “sees” the infrared ink, and “translates” it into a black & white image that can be displayed on an LCD, LED or other viewing screen or monitor.

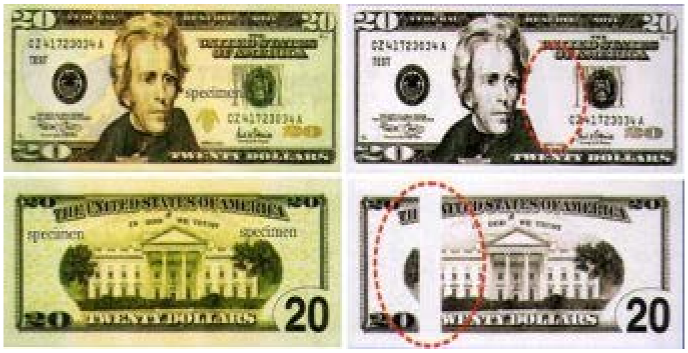
IR features are widely used on many different types of documents. Many world currencies and national and international identity documents include IR inks for security.

Though advances in printer and toner technology has allowed counterfeiters to overcome many of infrared printing’s advantages, IR still poses several challenges to counterfeiters, making it an effective security methodology.



One major advantage is IR’s ability to be rendered into “machine readable” characters or features that allow for automated validation by a machine, such as a bill acceptor on a vending machine, or a high-speed money counter. The image above shows the appearance of a U.S. $5 bill under infrared light. The two “bars” are precisely located and can be easily seen and read by machines.

It’s amenability to machine-reading notwithstanding, we score IR rather low as an effective technique as a point-of-transaction security tool. The simplicity and ease with which a machine can validate IR features works exactly against the human employees who need to verify the feature with their own eyes. It is easy to grasp the difficulty in teaching employees how to distinguish between the $20 note, seen here, and the $5 note previously pictured. In addition to the difficulty of training employees, the equipment needed to view these features is both bulky and expensive.



- **Magnetic Character Printing –** Magnetic ink is used to print machine-readable characters that help automated devices identify and authenticate documents. These characters can range from quite simple codes (for example, the U.S. $5 bill is imprinted with a dot-dash-dash-dot symbol) to very complex, such as the characters printed on checks (MICR) or on passports (B900) in which names, addresses, account numbers and other important information can be communicated.

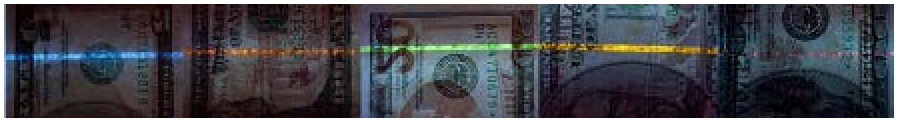
  At one time, magnetic printing posed a significant barrier to counterfeiters, however, this no longer holds as true. While it is still difficult to produce complex magnetic features that can accurately recreate the B900 printing on passports (this information is encoded and requires decoding “keys” in order to be read), it is fairly easy to create the simple features seen on banknotes and personal checks. MICR printers are easily purchased on the Internet.

Magnetic printing still offers a modicum of security on these simpler documents, as many of the counterfeiters dabbling in fake money don't even bother to add the magnetic ink to their bills. Thus, while conducting a simple test for the absence of magnetic ink can detect some counterfeits, its presence on a banknote or personal check by no means assures that it is genuine.

- **Ultraviolet Inks –** The opposite of infrared, ultraviolet wavelengths are shorter than the human eye can observe. The result is the same; these inks require exposure to light sources that fall outside of the human visible spectrum in order to be seen. However, the way ultraviolet ink reacts to UV light differs greatly from how infrared inks react to an IR light. UV inks, when excited by the proper wavelength of ultraviolet light, will produce a fluorescent response that is visible to the human eye. No filter or imaging viewer is needed to see the reaction of the ink to UV light.

  Because we can "see" the covert marking when it is properly excited, and because UV ink is itself invisible under ambient light, ultraviolet security features are used extensively to protect financial instruments and identity documents:

  - Currency notes (US dollars since 1996, most other world currencies)



  - Passports and national I.D. cards
  - Credit, debit, stored value and gift cards
  - Cashier's and traveler's checks
  - Social Security and voter registration cards
  - Casino chips

Printing with UV inks poses some technical challenges to rank & file counterfeiters who use digital printers to produce their counterfeits.

For instance, the compounds used to create UV fluorescence ("fluorophores") are volatile and evaporate quickly unless they are locked into a neutral molecule. The U.S. Bureau of Engraving and Printing adds fluorophore to the Teflon used to make the security strips embedded inside currency. So, even if counterfeiters print a UV feature, it likely will wear off shortly. As with many other security features, forgers often do not even attempt to replicate ultraviolet features. They either do not know UV features exist on genuine documents, cannot master the technique to use UV or simply pass their fakes at locations that do not test for ultraviolet markers.

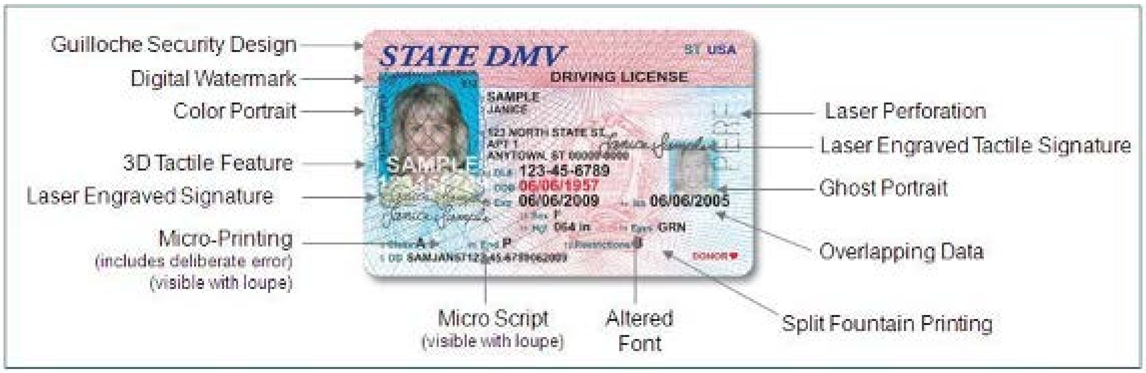
We consider the UV feature highly valuable as a security authentication method. In terms of its absolute security, it is not impossible to overcome the printing challenges, and some very professional counterfeiting operations have been able to replicate the features ("superbills" and government-sponsored fake I.D. programs have managed it). However, the flexibility, ease of use and relative low-cost of the equipment required to authenticate UV features at the point of transaction make it a viable option for use in many different situations – from small businesses to large enterprises.

Scientific Analysis

As we progress up the scale of accuracy and complexity in document authentication, the third general technique makes greater use of forensic analysis. That is, valuable and sensitive papers are examined and compared to samples known to be genuine. When the presented banknote, passport or other document deviates from the expected value, additional inspection is warranted.

Pattern Matching

With pattern matching, the idea is that a document can be compared against a library of known features and designs to determine whether it is genuine.



Pictured here is a rendering which shows the number and diversity of different security design elements that may be included in a single secure document design. While this is not a comprehensive listing of such features, note that one document may contain dozens of individual design features that can be used in a pattern-matching application.

To verify the pattern of any given document, an intelligent library, or database, is built and continually updated to provide a set of templates against which any document presented can be compared. Hardware devices then capture images of the document being tested, which are run through the database to identify what type of document is presented. Then, the software compares the document images to the database of authentic templates of that specific document-type to arrive at a level of probability that the presented paper is genuine.

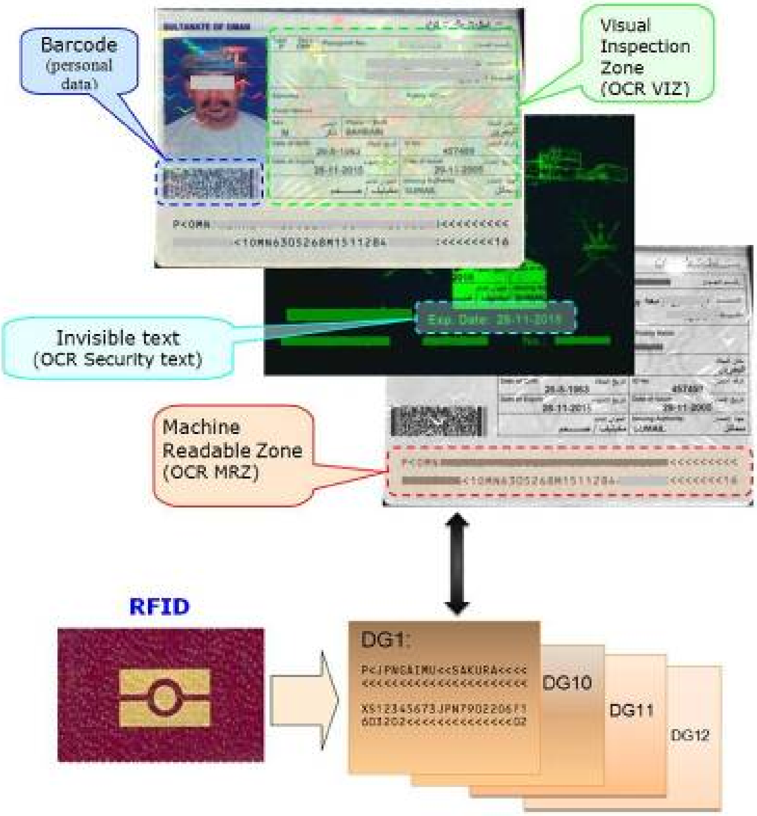
Law enforcement uses a similar technique for comparing fingerprints to those in a database. The more data points that match, the more likely it is that the print left at a crime scene belongs to the individual attached to the known sample.

Almost by definition, the accuracy and reliability of this technique produces a very high level of confidence that counterfeit documents can be detected. The more complex the document (and the more complete the library used to match patterns) the greater will be the probability of correctly authenticating a given document. Using machines that compare only three or four elements when trying to verify currency notes probably will achieve lower accuracy levels than devices that validate I.D. cards, which may have 20 or more features to compare.

Data Comparison

The underlying strategy for how to authenticate a document using data compare fundamentally differs from that for pattern matching. With pattern matching, the assumption is that "we know what the document should look like, so let's see if it matches". Data compare, on the other hand, is focused on gathering pertinent data from the document itself and comparing it to see if it all agrees with itself.

Multiple techniques are available to extract data from a document. Some we have already discussed, such as reading magnetic ink, or looking for identifying patterns printed in infrared. We briefly touched on the idea of B900, which is an international standard format for printing machine readable zones. Other techniques may include optical character recognition, which is a software capability for reading the printed information and translating it into a digital format.


Barcode (personal data)
Visual Inspection Zone (OCR VIZ)
Invisible text (OCR Security text)
Machine Readable Zone (OCR MRZ)
RFID
DG1:
P<JPNGAIMU<<SAKURA<<<<
X512345673JPN7902206F1
DG10
DG11
DG12

Sophisticated documents, such as passports and national I.D. cards may contain barcodes, magnetic storage media ("magstrips"), contact chips, contactless RFID chips and more. After identifying the document type, "data compare" devices will first look to see whether all the expected forms of data are available. Then, they will proceed to extract all the available data and put it into a table so it can compare the data content in each security feature.

Each of the above listed methods for storing information will have many fields that overlap - "first name," "document number," "expiration date," etc. The software will compare the data from each of the different sources and make sure they all agree. If discrepancies are found, the user interface will warn the user that there are problems with the data and the document may have been tampered with.

Tools for Counterfeit Document Detection

Available tools for counterfeit detection and document verification run the full spectrum, from products that are so simplistic they are worthless, to convoluted to the point of being impossible to use. The best tool for the job depends entirely upon the situations in which they will be used. The physical limitations –light, space, time, etc. – must be considered along with the type of documents to be checked, the likelihood of encountering fakes, the consequences of not detecting them, and more.

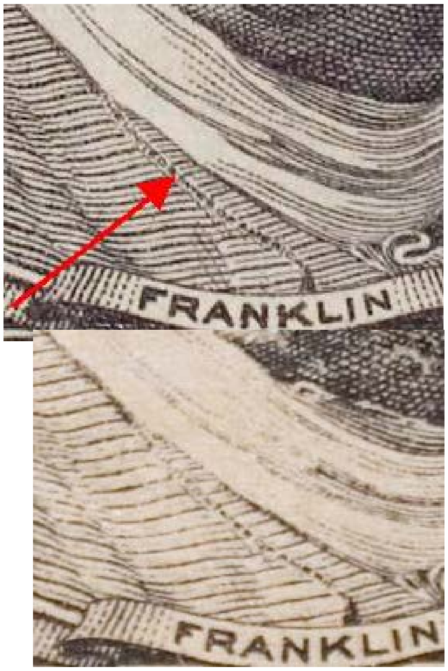
We have segmented the types of authentication tools into into two primary categories: Visible Verification and Forensic/ Machine Readable/ Pattern Matching Devices. Visible verification relies on “human decision” to make an authentication. Devices in this category all require a person to confirm that they see the proper security feature. The other category includes machines with software algorithms that tell operators what they detect and do not necessarily require a person to make a determination themselves.

The following discussion is not intended to be an exhaustive review of all possible products and devices, but rather an overview of the types of device available. Users are encouraged to perform further research, considering the variables mentioned above, to choose the right device for their situation.

Visible Review Aids

These devices are designed to aid the user to see and verify the covert features that were discussed in a previous section of this paper. These devices do not have built-in logic to reach an authentication determination by themselves. Instead, they help the reader find and authenticate the covert security features placed in currency and documents. The user is the final arbiter. Can he or she see the markings and determine that they are genuine?

- **Magnifiers and Jeweler’s Loupes –** Magnification aids viewers in seeing and analyzing microprint on documents. Jeweler’s loupe is a specialty type of magnifying glass originally developed for examining precious stones. They are also well-suited for reading the tiny, fine print used for security on banknotes. Because microprinting requires advanced offset printing techniques, many counterfeit documents either do not contain any microprinting, or the quality of the printing is so poor that it is easily identified when viewed under



magnification. In fact, the magnifier can be used to view any fine-line details produced in higher-level offset or intaglio printed documents. As the images to the right show, the genuine document (top) contains clear-to-see printing in the collar and very fine-detailed lines elsewhere, while the digitally reproduced copy (bottom) is unable to mimic these features accurately.

PROs -- Because microprinting itself is a relatively high-confidence security feature, only the most advanced counterfeits are able to reproduce the feature such that it can withstand the scrutiny magnification allows. Thus, if microprinting is verified, then it is quite probable that the document is genuine.

CONs – Subjecting a bill to apparent microscopic analysis in the presence of the person submitting payment is bound to put a damper on the customer experience. There may be some environments where having someone bending over your document with a magnifying glass would not be offensive, but in most retail/hospitality/financial service circumstances, this would not be the case. Second, the teller or cashier must know what to look for. In some cases, this may not be too difficult to train. Finding and authenticating the microprinting on $50 and $100 bills, for example, can be taught in minutes. However, every jurisdiction that distributes identification cards and every company that sells traveler's checks has its own set of microprints and specific document locations where they are located. Verifiers would need to remember a broad library of features.

These negatives makes using magnification an unfeasible option in many circumstances. Finally, although they comprise only a small percentage of the counterfeits in circulation, there are some fake documents – usually produced in collusion with certain unfriendly governments – that DO contain appropriate micro-printed features. Magnified review will not detect these counterfeits

- **Infrared Viewers** – As discussed in the previous section, products are available that allow a transaction-counter employee to view documents under infrared light. Devices such as the one pictured to the right, use infrared light sources to activate the IR inks, and then render that imagery into black & white on an imaging display screen.

  PROs -- Most counterfeiting operations neglect to include IR ink in their fake documents. Point-of-sale employees who know what to look for, can easily detect their presence and determine a bill is genuine.

  CONs – Unfortunately size and cost of the equipment needed to view the features. Devices such as the one pictured here can easily run $200 to $400, and take up a square foot of valuable counter space. In addition, infrared features used in most documents are not intuitive or easy to remember. U.S. dollar notes, for instance, feature single or double bars, while on many I.D. documents, only certain parts of the text printed on the surface will be visible under infrared light. Ultimately, the IR ink features are better left to machines that can be programmed to look for specific IR markers, and do not require the size or expense of an imaging screen in order to function. Many high-speed money counting machines and currency validators employ IR ink testing as one of several validation tests for banknotes.

- **Magnetic Ink Detectors –** The idea behind magnetic ink detectors is fairly simple. Many secured documents included printing of "invisible" magnetic ink character sets that can be decoded by devices designed to read them. This MICR (magnetic ink character recognition) technology is another commonly used by bill acceptors and high-speed counting machines to identify and differentiate banknotes. The logic behind using magnetic ink as currency validation technique at the point of sale is based on the belief that if a device can detect the presence of magnetic ink on a banknote the bill must be genuine. Proceeding with this fallacy, numerous manufacturers have produced low-cost (as low as $5.95, in some cases) tools designed for a cashier or teller to manually trace across the surface of a banknote. When the machine detects a magnetic field, it will indicate, with a light, a tone or some other method, notifying the user that the magnetic feature is present.

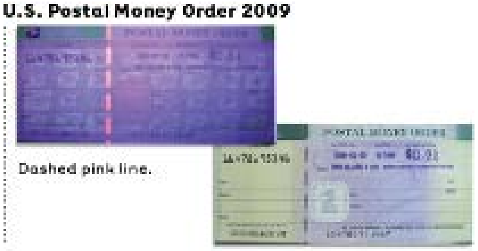
PROs – Their low cost and ease of use may make magnetic ink detectors seem an attractive option. Simply rub the head of the tester around the banknote and look or listen for the indicator to tell you it is a good bill.

CONs -- Unfortunately, the logical foundation behind the use of these devices is flawed. Everyone would like to think that a $6 tool can detect counterfeit currency, but the reality is that this test will do nothing more than detect counterfeits produced by absolute amateurs. As discussed earlier in this paper, in recent years, there has been a steadily rising trend of counterfeiters bleaching or "washing" low denomination banknotes and reprinting them as counterfeit $50 and $100 bills. Washing notes often maintain their magnetic features, tricking magnetic ink machines and their users with false-positive readings that indicate that the bill is genuine even though it is not. In addition, a simple search of eBay or Amazon reveals dozens of vendors selling magnetic printers, and many of the major printer manufacturing companies produce magnetic ink cartridges for their printers. In addition, the "supernotes" produced by foreign governments do contain magnetic ink characters. More problematic are the range of devices purporting to be "advanced" bill detectors, which do nothing more than give a "red" or "green" light to indicate whether a bill is false or genuine. Models currently marketed in the U.S., such as the D450 and the CashScan are guilty of this deception. These devices do the same thing as the little $6 device pictured above, but they are priced at $99 to $179!

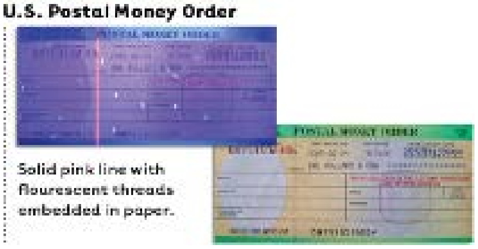
- **Ultraviolet lights** – As with infrared and magnetic ink, ultraviolet ink printing is present on many documents, appearing only when they are viewed under the correct wavelength of UV light. The makers of such documents have placed the features there precisely so that they can be used as a verification technique. Upon exposure to an appropriate UV light source, the ink feature becomes visible to the human eye, without the need for any additional tools. In this sense, UV inks really are designed as a "human-readable" security feature, whereas IR and magnetic inks are designed to be machine-readable only.

PROs – UV lights are among the lowest-cost solutions available in the market, making them affordable for point-of-transaction authentication at even the smallest restaurant or retail outlet. They also are simple to use, requiring little cashier training. Simply place the bill or ID document under the UV light and verify that the special ink appears. A wide variety of documents in addition to currency make use of UV security features, so using this verification measure offers a one-stop solution for checking traveler's checks, driver's licenses, passports, credit cards and more. A tried and trusted technology, for more than a half century ultraviolet ink has been a globally accepted method as an effective strategy for securing documents.

U.S. Postal Money Order 2009



U.S. Postal Money Order

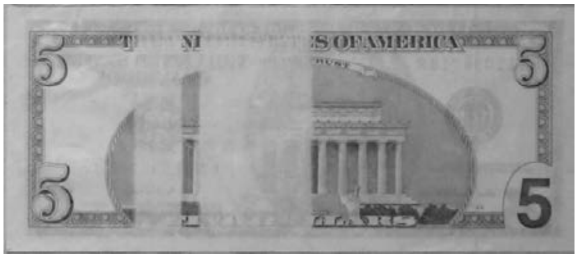


CONs – Like other visible verification techniques, UV authentication requires a person to interact with the document and positively confirm that he or she sees the proper UV security feature. While this may seem simple enough, many organizations do not wish to delegate this type of decision making to the transaction-level employee, where inattention or incomplete training can produce confusion and inaccurate results. If employees have not been told what to look for, or haven't been provided with proper materials for reference and comparison, they could easily decide that they have received a genuine item when, in fact, it is counterfeit. For example, when exposed to UV light, a "washed" $5 bill, which has been bleached and counterfeited as a $100 bill, will display the blue $5 security feature inserted when printed by the Bureau of Engraving and Printing. Legitimate $100 bills display a red UV feature, so the blue stripe would be a dead giveaway to a properly trained and attentive employee. Boredom or inattention, however, may cause the cashier to register that UV ink is present – failing to comprehend the significance of the color – and pass the bill as real.

Finally, while difficult to counterfeit, UV features are by no means impossible to reproduce, making it possible for counterfeit documents to elude this level of scrutiny.

Advanced Analysis Devices

Advanced analysis devices are machines that read the many different covert or latent security elements placed into documents. In the previous sections, we have discussed IR ink, magnetic ink and UV ink printing as means of “visible” verification. Each of these printing techniques can also be used to create mechanically or digitally read patterns, designs or characters serving as specific identifiers of a document type.



This image of the $5 U.S. banknote under the an infrared light shows two clear bands that can be used as a basis for identification by an intelligent device, programmed with logic noting the proper locations and dimensions of this feature. Similarly, the IR features of the other denominations of US banknote would be programmed into the device. If the presented bill matches these parameters, it passes.

Magnetic ink can be used to print actual characters which magnetic reading devices can detect and decipher. If they match the “known genuine” markings in the machine’s database, the bill is good. Other features, such as metallic threads, metallic inks, clear polymer windows, intaglio printing features, colors and other controlled attributes can also be identified by intelligent scanning devices.

Currency Detection

The marketplace is flush with devices designed to read machine readable features on currency notes to identify them as genuine. Buyers should be cautious before purchasing such devices that rely on only one type of MRC read. For example, those machines that only check for the presence of magnetic ink, or look only at infrared printing before giving the green light. Instead, care should be taken to choose devices that test for multiple features and then cross-check the results to ensure that authentication will be reliable. Devices that read infrared, magnetic, ultraviolet, intaglio and other features in combination will be much more difficult for counterfeiters to defeat.

Bill Counter
with
Counterfeit Detection

Identity Document Detection

Identity documents are also frequently provided with machine-readable information that can be used to identify them. These can be in many forms, including 2-dimensional bar-codes, magnetic tape, contact chips, RFID chips, digital watermarks, and more.

Actual I.D. authentication requires a device that is capable of reading and comparing data from multiple sources or comparing the details of security features included on the I.D. document itself. However, the MRC readers that function on I.D. documents can extract data from the document and subject it to software that collects and tabulates different results, such as age verification, visitor management, or maintaining records for compliance purposes.

- **Data Compare Devices –** Data compare devices take the concept of MRC to the next level. Unlike the previously described devices, which may read one or two Machine Readable data sets from a document, the data compare device will identify the document type (e.g. “California Driver License” or “€50 banknote”). The data compare software will know that on this document type, a given set of MRC data should be available.

  It will then search for that data, whether by reading basic printed features, more advanced digital security features, barcodes, RFI.D. chips or whatever else may be included in the document.

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

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

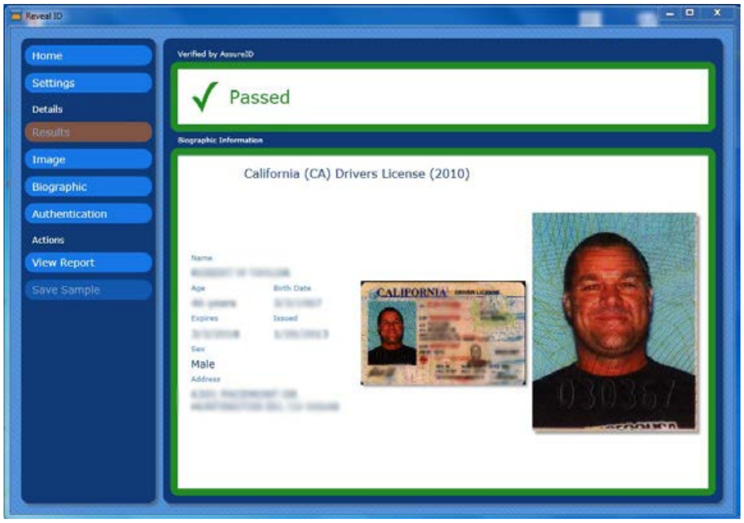
- **Pattern Matching Devices –** Pattern Matching is a different sort of document analysis. Rather than reading data from the document and determining what it says, pattern matching attempts to determine whether the document itself is “built” properly.

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

- **Hybrid Pattern Match/Data Compare Devices –** The most successful and highly accurate document verification tools typically combine some hybridization of the above-described techniques. These devices include information, software, and imaging technologies that make them effective tools not only for document authentication, but also for data extraction and storage.

  One example is the AssureTec I.D.150, pictured to the right. This hybrid device mechanically feeds a standard international driver’s

license and national I.D. card design and formats. The I.D.150 reads bar-code and/or magnetic strip data from the I.D. document, then conducts some pattern matching tests (e.g. IR and microprint examination) to validate the document. It is able to extract data and images of the I.D., and will alert the user to any potential issues with the document.



✓ Passed

California (CA) Drivers License (2010)

Name
[illegible]
Age
[illegible]
Birth Date
[illegible]
Expires
[illegible]
Issued
[illegible]
Sex
Male
Address
[illegible]

To the left is a screenshot of one software solution, Reveal-ID, that works in combination with the ID-150 (and other scanner-hardware devices) available for conducting this type of data matching and pattern matching ID document authentication. Reveal-ID can conduct several dozen different forensic-level authentication tests of a document and assign a pass or fail grade to the document

Another device that fits this final category description is the Penta document authenticator. The Penta is able to “read” ID-1 documents, passports and other global I.D. formats. Because the company that makes the authentication software manufactures many of these global documents, their pattern matching “library” is extremely robust.

The Penta unit is, in fact, a high-resolution camera which has built-in light sources that allow it to capture document images in IR, UV and white-light. These images are compared to its document library and high-confidence document authentication can be performed. This machine is also equipped with RFID and smart-chip readers to capture the information stored on them. The Penta is capable of reading MRZ “zones” standard to ICAO document formats, and is B900 ink-capable. It can read mag-strip and bar-code data, and is also capable of conducting OCR reads of the printed information. In other words, the Penta captures almost every single element available on the document, from which it conducts a combination of pattern-matching and data-compare tests for nearly foolproof verification. The results are configurable so that a complete record of the document investigation can be saved to an encrypted file, including images of the document and archived for later retrieval.

Multi-Layered Approach to Fraud Detection

Addressing the multiple points of potential vulnerability to fraud loss and I.D. verification-related regulatory compliance violations requires a systemic approach to risk analysis. Modern business organizations may encompass diverse activities, including physical store operations, finance departments, “covered” financial transactions, sales of controlled products and acceptance of a broad range of payment types. Each activity must be evaluated with an eye toward scope, type and depth of risk at each point where the organization conducts a public-facing transaction.

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

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

The “Displacement Effect”

This is a phrase FraudFighter coined after hearing the same observation from numerous customers. We have frequently found companies willing to address their “problem fraud stores” by placing our equipment into the stores where they are experiencing the highest levels of fraud. Afterwards, the LP staff would relate that problems in the stores with FraudFighter equipment had virtually disappeared, but the stores that previously had no problems were now showing signs that the criminals had focused their attentions on them because they didn’t have FraudFighters. For LP managers who were given bonuses based on improved fraud numbers, those who had our equipment were at a distinct advantage over their peers! This “Displacement Effect” underscores an important fact about fraud prevention. Criminals will exploit any weakness they can find. Layered solutions help to plug the vulnerabilities.

Multiple Points of Vulnerability – A Case Study

No two organizations are alike. Even companies operating in the same industry, geography, price point and target market will have unique security requirements and different exposure tolerances to different varied vulnerabilities. Similarly, no two points of transaction are the same. For this reason, it is not advisable to force an out-of-the-box solution to meet the needs of a company without first understanding what problems and potential vulnerabilities exist.

As an example, FraudFighter has consulted and provided our solutions to the challenges facing a large grocery store chain. Our initial understanding of the company’s business environment was that this type of operation performed a high-volume of relatively low-value transactions with a transient customer base. On average, the stores operated 13 cash-wrap locations. Accordingly, the initial customer-driven discussions were focused on the need to validate payment forms and to verify I.D.’s for alcohol and tobacco sales.

However, after learning in detail about the operations, we discovered that some of the greatest operational problems experienced by the client were associated with the “covered” financial transactions they conducted. Sales of money orders and electronic funds transfers to both domestic and international destinations triggered a slew of regulatory compliance issues and reporting requirements. One Southern California region alone, had endured more than 25 separate IRS audits in one quarter in connection with the sale of money orders and wire transfer services. In addition, the sale of PPA compounds (AKA, ephedrine, a key ingredient in methamphetamine production) and the operation of a pharmacy also created the need to log and record identities of some customers.

FraudFighter proposed a multifaceted approach to address these vulnerabilities. At the cash-wrap locations, basic counterfeit detection devices (i.e. UV devices) are installed. At the customer service counter where money orders and wire transfers are processed, UV devices are installed alongside image capture devices to collect and securely store images of I.D. documents presented in order to comply with Red Flag, Customer Identification Program and Know Your Customer requirements. The same image capture device at the customer service counter is used to log I.D.’s for purchase of ephedrine products. The customer service desk also uses an electronic currency verifier to quickly scan high-denomination banknotes presented at the time money orders and wire transfers are purchased.

At the pharmacy, a separate image capture unit logs medical cards and I.D. documents for all purchases of Class I narcotics. Finally, in the back-office, the FF-1000 quickly double checks on cash-drawer reconciliation counts.

Conclusions

The statistical evidence is quite clear: Counterfeiting of valuable documents is on the rise. Whether we consider the counterfeiting of currency, identity documents, negotiable instruments, credit cards, title documents, certificates, coupons or any other document that conveys value to the holder, the trends in desktop publishing technology advancement and international organized crime involvement have created an environment rife with forgeries of all document types.

Losses experienced by commercial organizations as the result of these crimes are astounding. Approaching $1 trillion globally each year, when all types of counterfeit fraud are included. When the additional social, productivity, punitive and other “soft costs” connected with such loss events are factored in, the damage to the economic health of any organization exposed to such fraud can be devastating.

Organizations experience not only direct financial loss as the result of counterfeit fraud, but under certain circumstances, also face stringent compliance regulations that require them to conduct and record a document authentication at the time a transaction occurs. Failure to do so may expose these organizations to significant administrative and criminal penalties. Most valuable documents do contain one or more security features designed to enable verification or authentication by the recipient. The nature of such security features vary, from the simple to the complex. The type and variety of such features is broad, but not unlimited.

Specialty companies have responded to the long-term issues inherent in counterfeit fraud with products that enable organizations to conduct the document review needed to confirm the presence of security features. More advanced equipment will not just verify the existence of the security feature, but will also validate it as genuine - containing the proper attributes, and thus can provide assessments with greater accuracy. At the high-end of the document authentication scale are those products capable of reading encoded information and comparing the design and layout of specific features in the document to provide a definitive answer, including probability that the document is genuine.

Deciding which of these products an organization should use requires an analysis of the organization’s exposure to different types of fraud during the different transaction types the organization conducts during the course of business. Most organizations would ultimately benefit from the design of a “layered” counterfeit detection program in which lower cost “basic” testing is conducted at the low-risk locations, while higher-end (and higher-cost) equipment is used in those locations where the risk exposure justifies the investment.