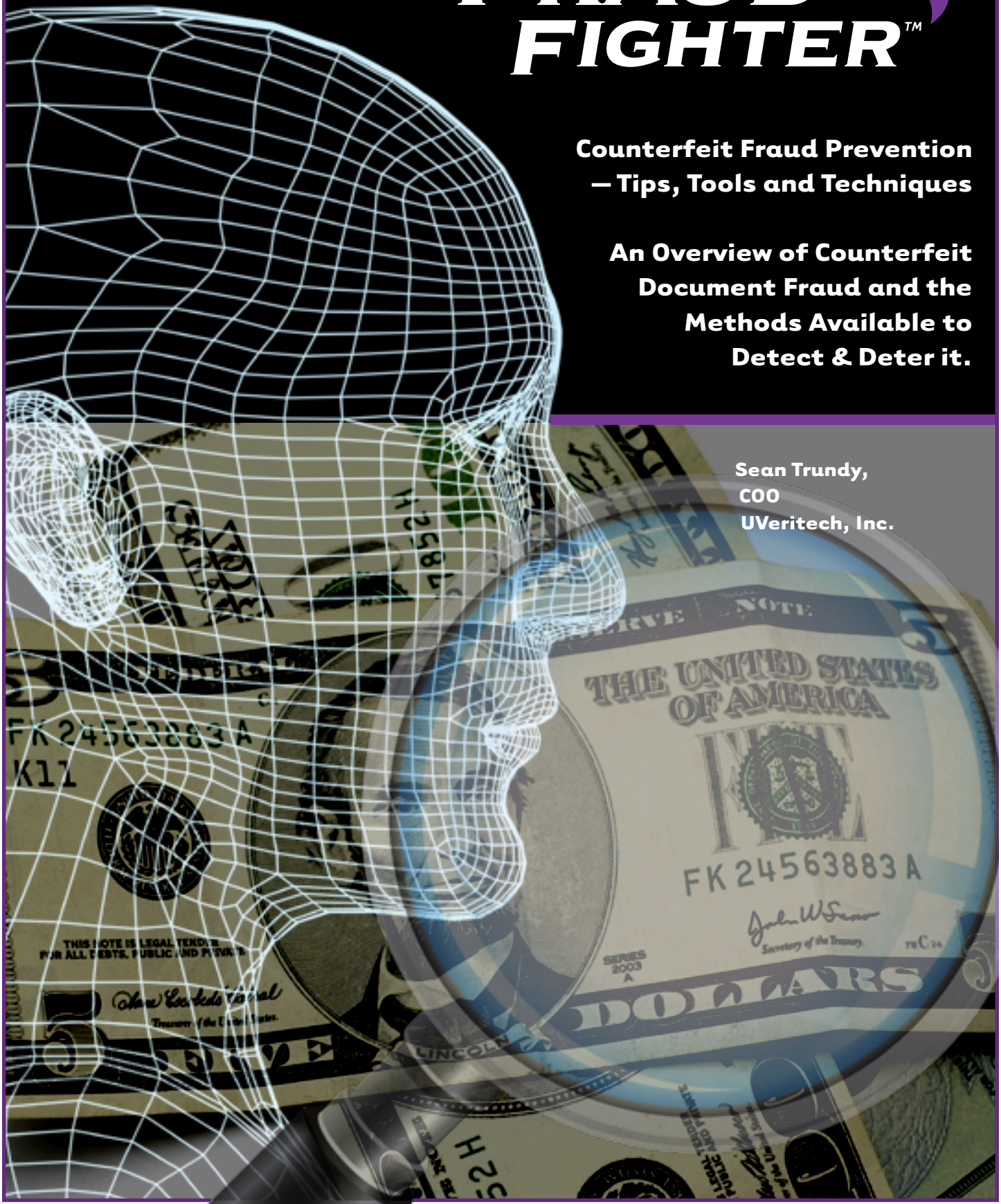
UVeritech

Supplier of Fraud Fighter™ Products

FRAUD FIGHTER™

Counterfeit Fraud Prevention — Tips, Tools and Techniques

An Overview of Counterfeit Document Fraud and the Methods Available to Detect & Deter it.



Sean Trundy,
COO
UVeritech, Inc.

1743 South Grand Ave., Glendora, CA 91740 www.**fraudfighter**.com 800.**883.8822**

Contents

Introduction

Worldwide financial losses resulting from counterfeiting have been significantly on the rise. Growth trends for criminal fraud of almost every type have shown a steady and consistent pattern of year-over-year increases. This is particularly true when one looks at recent behavior associated with the use of forged documents. A combination of technological factors has led to the increased capacity of non-professional counterfeiters to become successfully involved in the crime of forgery. This, in turn, has caused an increase in the number of operations creating counterfeits, with the run-on effect of making it far more difficult for law enforcement organizations to combat the trend.

Public-facing organizations, regardless of their nature, face a complex variety of activities they must carry-out with their constituents. Whether performing financial transactions, validating identity in order to conduct business, or accepting a broad array of different documents in order to establish a relationship, the burden on the transaction-level employee to be able to recognize and authenticate potentially thousands of different documents is too great to be performed reliably. Thus, organizations of all types are exposed to potential loss from this increasingly common form of fraud.

Forgery may involve a surprising variety of different document types. At the core of the criminal forger's strategy is to replicate a document that conveys some value or benefit to its holder. Therefore, any document that has intrinsic value may be counterfeited. Most common are currency notes and identity documents.

The need to detect and prevent forgeries is of vital importance to any organization. Not only are the losses that may result from counterfeit fraud harmful to financial health and profitability, but in many cases, the legislative environment regulating certain types of transactions can potentially create exposure to punitive losses in the form of fees, penalties and criminal or civil litigation should an organization fail to properly validate documents during a transaction.

The present document seeks to provide an overview of document counterfeiting and discuss the methods and tools available to aid organizations in detecting forged documents at the time they are being presented.

Counterfeit Fraud

Mention the word “counterfeit” to most people and one of two things typically jumps to mind: either “Counterfeit Money” or “Counterfeit Products”, (e.g. fake Gucci bags or Rolex watches). We will seek to expand on the topic of counterfeit fraud, and more specifically, the category of crime involving the presentation of fake or counterfeit negotiable instruments.

For the purpose of this document, we will define the term counterfeit fraud as:

“The act of intentionally presenting a forged item in order to gain a benefit.”

While often associated primarily with currency, in fact, this behavior can include a wide range of items, including:

- Negotiable instruments (cash, checks, cashiers checks, postal money orders, traveler checks, gift certificates)
- Identification Documents or “breeder” documents to create a false identity (e.g. birth certifi cate, driver license, passport)
- Title documents showing ownership (vehicle, real estate)
- Certificates of Authenticity for collectibles and rare articles
- Coupons, “promotional dollars”, or other store currency
- Credit cards, gift cards, P-Cards, stored value cards, debit cards

Counterfeit Currency

It is said that currency counterfeiting is one of the oldest crimes in human history. Ever since people began trading goods and using coinage, others have been attempting to pass fake, lower-value versions of the currency in an effort to gain advantage.

In the United States, counterfeiting has had a consistent presence throughout the history of the dollar regime. During some periods of the 19th century, counterfeiting was so prevalent, much of the country refused to accept the paper “legal tender”, which was produced by as many as 1,600 different banks. After the formation of the US Federal Reserve Bank, in 1863, currency manufacturing was centralized, and a common currency was created. However, this didn’t stop the counterfeiters. In fact, after the Civil War, with a reported one third of the currency in circulation being counterfeit, President Abraham Lincoln created the Secret Service with the mission of suppressing currency counterfeiting in the United States.

The Modern Face of Currency Counterfeiting

Offset Printing Counterfeiters

Throughout most of the 20th century, the techniques for counterfeiting U.S. currency remained unchanged. Using photographic plates, stencils, and offset printers, counterfeiting required the advanced skill-set of the professional counterfeiter, who over the years would perfect his craft in an attempt to overcome the security features of U.S. currency. Primary among these is the printing method of money itself, the "intaglio" process, where heavy presses force ink deep into the paper, to create the distinctive "raised" feel that is recognizable to anyone who regularly handles U.S. banknotes. Offset printing can only imperfectly re-create such an effect but, with care, the result is often good enough to pass.

Many additional security features, from intricate scrolling to the use of both green and black ink to the use of special paper, have typically presented challenges for all but the most determined counterfeiter. 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 fluorescent inks that are difficult to work with. Many counterfeiters omit these features altogether.

Traditionally, after producing an acceptable copy, the counterfeiter would repay his efforts by producing large quantities of the counterfeit note, then face the difficult task of circulating them, normally leaving a trail both forward to his colleagues who received the counterfeits in bulk, and backward to the supplier of the special inks and paper. The difficulty of hiding such large-scale activities regularly led to tips gathered by law enforcement, whose historical success in seizing fake money prior to its circulation has been exemplary.

Digital Counterfeiting

Today, counterfeiting requires a much smaller initial investment and, consequently, a smaller amount of product to make it profitable. A good color scanner, computer, and laser-jet printer, capable of producing passable-quality color copies, can be had for about $1,000.

This lower threshold not only allows someone to print counterfeit money secretly at home, but also frees them from the need to rely on others to launder large amounts of counterfeit bills. Thus, even though digitally reproduced counterfeits tend to be lower in quality than offset notes, they are less likely to be seized and more likely to be passed into circulation. According the Counterfeit Division of the Secret Service, the last decade has seen proliferation in digital counterfeiting by street gangs and links with the drug trade.

The cumulative result has been an explosion in the number of counterfeiting operations, each producing a relatively small quantity of fake money, good enough to be passed at retail outlets. No longer able to rely on the seizure of large blocks of cash, the Secret Service has seen its domestic seizure rate fall steadily, from 70 percent in 1995, to less than 20 percent today. Accordingly, a growing number of counterfeits are being passed on to the public.

Organized Crime Involvement

In addition to the rise in home-based digital counterfeiting operations, a second key contributing factor to the increase in counterfeit currency is the involvement by international and domestic crime families in counterfeiting. The three following stories illustrate this;

- In 2007, US government documents revealed that a Bulgarian crime family has been closely tied to the distribution of Syrian government-produced "superbills". These Bulgarian mafia figures are able to act with impunity within their own country, and utilize a complex global distribution network to circulate the counterfeit bills in Europe, South America and the United States.
- In 2008, a three year investigation by InterPol, Scotland Yard and the FBI resulted in the convictions of 18 people involved in an international counterfeiting ring responsible for passing over $40M in counterfeit Pounds, Dollars and Euros in a one-year period.

- In 2009, Wilson Liu, a Taiwanese national responsible for bringing as much as $25M in U.S. "supernotes" into the U.S. gave evidence to the FBI in which he implicated the involvment of Chinese and Russian Mafia families in the dissemination of North Korean supernotes. North Korea, it was revealed, manufactures counterfeit U.S. currency and uses it as the currency needed to acquire parts and materials in the international marketplace necessary for its nuclear weapons program.

Recent news stories have also closely tied U.S. organized crime to the 2010 "epidemic" of Peruvian counterfeits seen spreading from Miami to the rest of the country.

Crime organizations offer a key element missing from most counterfeit manufacturing operations – e.g., distribution. While there has been an enormous increase in the number of small home-based digital counterfeiters, the large scale manufacturer still does exist, and they have taken the digital techniques to new levels of sophistication and skill. Professional counterfeiting factories operated by international mafia groups are perfecting digital counterfeiting. Using production quality management processes such as Six Sigma, they produce consistently high-quality fakes, and are able to learn and improve from each consecutive production run.

At the higher end of the quality spectrum are some of the counterfeits made overseas. Foreign counterfeits — which are still predominantly made using offset printing methods and account for over 80 percent of all offset notes — have represented the majority of the total volume of counterfeit U.S. currency produced in four of the last five years. With two-thirds of the total U.S. currency supply held overseas, the $100 bill is more common abroad than it is in the United States. Perhaps for this reason, the most commonly counterfeited bill outside the United States is the $100 (domestically it is the $20).

How Peru Became the World's Counterfeit Capital

TIME

By Lucien Chauvin / Lima

Some of the best counterfeits come from Peru, which itself reportedly accounts for nearly 50 percent of all foreign-produced counterfeits. To avoid the problem of detection by feel, "Peruvian notes" are printed on bleached $1 and $5 bills that are then converted into $100s. The quality of these bills is extraordinarily high, and they are virtually undetectable by the average citizen. Smuggled into the United States, the Secret Service estimates that up to one-third of all counterfeit money in circulation domestically is Peruvian in origin.

Foreign Government Involvement in Counterfeit Currency

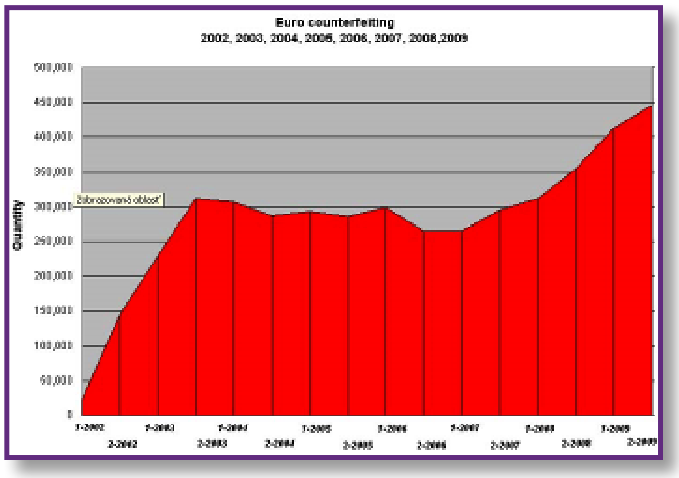
The best-quality counterfeits, however, are those that are produced using intaglio methods, on the identical presses used by the U.S. Bureau of Engraving and Printing. Given the expense of such presses, and their availability only from a single manufacturer in Switzerland, the Secret Service suspects foreign government involvement, by such countries as North Korea, Iran or Syria, in the production of these "superbills." Fortunately, the "pass rate" for counterfeit U.S. currency overseas is extremely low, as a result of its detection and seizure in large quantities before it goes into circulation. Still, even the Secret Service acknowledges that there may be radical underreporting of counterfeit U.S. currency being passed, given the diverse practices of law enforcement agencies and banks abroad. One encouraging facet of foreign counterfeiting, however, is that so far the number of foreign digitally produced notes has been miniscule, as computer technology has not yet penetrated as far as it has in U.S. markets.

Currency Counterfeiting on the Rise

The quantity of counterfeit bills in circulation has steadily risen over the past 12 years, and the rate of year-over-year growth has also been on the upswing. As the chart to the right shows, from 1999 through 2006, in the United States "confiscated" counterfeit currency increased from $39.2M to $62M. This 8-year period experienced a 55% increase, or an average increase of roughly 7% per-annum. However, starting in 2004, the advent of digital counterfeiting began to show its effect on these numbers, and the last three years on the chart show a much steeper slope, reflecting a faster rate of increase.

By 2008, over $103M of counterfeit dollars were confiscated in the United States, a 50% increase over the 2006 number. Then, in 2009, the number jumped up to $182M, a massive 77% increase in just one year.

This obvious trend is not difficult to see or understand. 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.



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 2009. 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 the most recent 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.

Types of Counterfeit Dollars

Digital Notes

The most ubiquitous type of counterfeit note circulated in the United States is the digital note - so called because the processes used to produce them involve the use of digital printing/scanning/graphics technology. In its simplest form, a genuine banknote is photocopied using a color copying machine. During the late 1990's and early 2000's, advances in photocopier technology made the ability to reproduce fine details and color combinations with high-level accuracy. This practice has, more recently, been undone by software installed on copier machines that is able to understand that a US banknote has been placed on the machine. The software is designed to shut-down the copier in order to prevent copies of the banknote being made. In some cases (depending on the model and type of machine), the copier will itself notify law enforcement that someone attempted to photocopy a banknote.

More common these days is the “Photoshop note” - e.g. a note that is scanned into Photoshop (or, another graphics program), and manipulated into a high-resolution image that can be printed on a color laser-jet or ink-jet printer. Again, the technological advances made on scanners and printers over the past 15 years has revolutionized this type of document counterfeiting. Scanner resolution has consistently improved to the point that all but the finest detail can be scanned into a digital file.

Printer toner technology has made great strides in just the last several years, making it possible for over-the-counter printers 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.

Washed Notes

Washed notes really could be treated as a sub-set of the digital note category, however, the widespread practice of “washing” bank notes as a counterfeiting technique has altered the US dollar counterfeiting landscape so greatly that we deal with it here as a separate category.

In essence, a washed note is any counterfeit that uses a genuine lower denomination banknote as the “paper stock” upon which the higher-denomination counterfeit is printed. Wily forgers realized that often their counterfeits were detectable by persons with years of experience handling dollars simply because the paper used for the forgery didn’t “feel” like real money. Also, 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.

To overcome this, counterfeiters use bleach or other solvent solutions to remove the ink from a $1 or $5 bill. They then print a digital replication of the $100 bill (or, in some cases a $50 note) onto the washed $5 bill using the above-described method of Photoshop and over-the-counter laser printers.

The resulting counterfeit note can be very difficult for the average individual to detect. Because the forgery is printed on genuine banknote paper, it will feel real because the paper is real. Similarly, the counterfeit ink pen will indicate a genuine banknote, because it is also simply testing the paper. Further, if the counterfeiter used a $5 bill as the base-stock, then the counterfeit note will have both a security thread and a watermark. While these will not be the correct thread or the correct watermark, many individuals who check for these features are simply looking to see whether it is present or not, and do not bother to validate that it is the watermark or thread that is supposed to be there.

Supernotes

Nobody is really certain who initially coined the phrase “supernote”, but the term has entered the vernacular now as a reference to any counterfeit banknote printed on the same (or similar) intaglio printing presses utilized by the U.S. Bureau of Engraving (BEP). One will also see reference to “super $100s”, “superbills” or “superdollars”. In any case, the concept is that counterfeit

notes are produced on equipment that is capable of reproducing the majority of the physical features of the genuine US banknotes.

The Secret Service, Interpol, Scotland Yard and other international policing agencies have determined that Supernotes are almost exclusively produced by foreign governments. This is because the type of specialized press utilized to produce the advanced security effects are too large and expensive for private sector counterfeiting operations to use. Also, the equipment used by the BEP is sold, exclusively, to government currency manufacturers and are not available for resale to the private sector.

The U.S. Government believes that these notes are most likely being produced in North Korea[1]. Other possible sources include Iran, Syria, Iraq and Nigeria. The name derives from the fact that the technology incorporated to create the note exceeds that of the original. Some have estimated that 1 in 10,000 bills is a counterfeit of the quality ascribed to supernotes[2].

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

Altered Notes

On the opposite end of the quality scale from the supernote is the last category we cover here – the altered note. As the name suggests, altered notes are genuine banknotes that have been altered to change their appearance. Of course, this is done to change the denomination / face value of the banknote. The common method for doing this has been to cut the four different numeric-corners off of four different 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 one dollar features, including clearly-printed text on both front and back reading "one".

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.

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

[2]"North Korea's Counterfeit Con". July 6, 2006. http://www.pbs.org/nbr/site/onair/transcripts/060706c/

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 (e.g. bars or nightclubs) 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 has the capacity to be counterfeited. The multitude of different types of document designed to deliver monetary value creates a long list of possible counterfeit fraud items. Consider the following list:

- Money Orders
- Postal Money Orders
- Cashier's Checks
- Traveler Checks
- State and Federal Treasury Checks
- Personal Checks
- Credit Card, Gift Cards, Stored Value Cards

Here is a variety of items that any business in the United States might, at some point during a typical day, require their cashiers to receive as a form of payment.

Unlike currency, which people often consider as suspicious, and which is commonly submitted to scrutiny when received, the above list of documents are often considered "safe". Traveler's checks, money orders and other secured checks are backed by the underwriting institution, which means that there is no fear to the recipient that there are insufficient funds to cover the obligation. Similarly, people tend to not worry about a state or federal check "bouncing". Because of this, people often "let down their guard" when receiving these forms of payment.

Money Orders

Most people think of money orders as "safe", i.e. – since it isn't a personal check, there is no danger of the money not being available when it is deposited. Unfortunately, it doesn't occur to most people consider the possibility that the money order is 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. Under these types of scam, which fall under many different guises, the con-artist tricks the victim into depositing a (counterfeit) money order and sending a part of the proceeds back to the fraudster. Whether the returned funds are a finder's fee, an "accidental overpayment" or some other detail, the end-result for the victim is that the counterfeit money

order is charged-back against the victim's bank account after it is discovered, and the victim loses either a) the face value of the money order or b) both the face value of the money order PLUS whatever property or good was sold to the bad-guy (e.g. a car or an appliance) and paid-for with the counterfeit money order.

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. 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 by the majority of people to be risk-free, due to the fact that 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, because the typical "common sense" practices one might use when receiving a payment from a stranger are often waived.

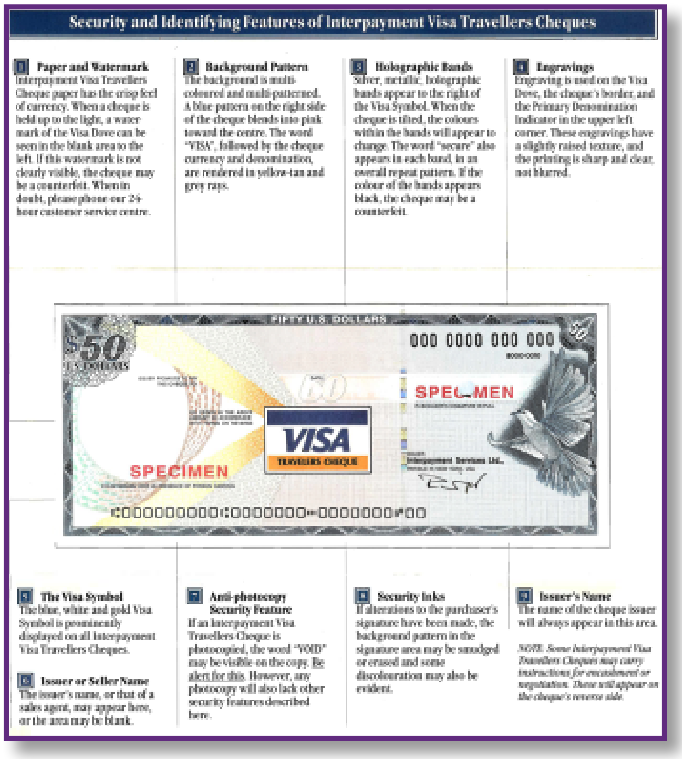
10 Weeks of Counterfeit Cashier's Check Reports to the FDIC

- 03/02 *American Security Bank, Newport Beach, CA* - Counterfeit Cashier's Checks
- 03/02 *Community America Credit Union, Lenexa, KS* - Counterfeit Cashier's Checks
- 03/02 *First California Bank, Westlake Village, CA* - Counterfeit Cashier's Checks
- 03/02 *First Savings Bank, Beresford, SD* - Counterfeit Cashier's Checks
- 03/02 *Lincoln Savings Bank, Cedar Falls, IA* - Counterfeit Cashier's Checks
- 01/03 *Central Jersey Bank, National Association, Oakhurst, NJ* - Counterfeit Cashier's Checks
- 01/03 *Delta Trust & Bank, Parkdale Parkdale, AR* - Counterfeit Cashier's Checks
- 01/03 *Frontier Bank, Davenport, NE* - Counterfeit Cashier's Checks
- 01/03 *Hedrick Savings Bank, Ottumwa, IA* - Counterfeit Cashier's Checks
- 01/03 *Metropolitan Bank and Trust Company, Chicago, IL* - Counterfeit Cashier's Checks
- 01/03 *South Georgia Banking Company, Omega, GA* - Counterfeit Cashier's Checks
- 01/03 *Stock Yards Bank & Trust Company, Louisville, KY* - Counterfeit Official Checks
- 01/03 *The Community Bank, Brockton, MA* - Counterfeit Official Checks
- 12/22 *Cashmere Valley Bank, Cashmere, WA* - Counterfeit Cashier's Checks
- 12/22 *Eagle Community Credit Union, Lake Forest, CA* - Counterfeit Official Checks
- 12/22 *First Chicago Bank & Trust, Chicago, IL* - Counterfeit
- 12/22 *Webster Bank, National Association, Waterbury, CT* - Counterfeit Official Checks
- Cashier's Checks
- 12/22 *First Farmers Bank and Trust Company, Converse, IN* - Counterfeit Cashier's Checks

Cashier's Checks are no less likely to be forged than a personal check. In some respects, they may even be MORE likely to be forged precisely because they don't receive the same scrutiny that a personal check might. The inset box on the right side of this page shows a recent 10 week period during which 20 different US banks reported to the FDIC that their Cashier's Checks were being 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 Checks

Despite the fact that traveler's checks are typically designed to be quite secure, counterfeits are prevalent. It is difficult to find statistics regarding this issue, but we have tremendous anecdotal evidence to suggest that it is a leading cause of cash register shrink at retail, quick service restaurant and banking establishments.



When surveyed by UVeritech, a cross section of over 300 respondent customers revealed that 79% of them had accepted counterfeit traveler's checks in the previous 12 months.

As can be seen to the left in this circular issued by Visa designed to educate cashiers, there are numerous physical (e.g. "overt") security elements contained within traveler check designs. The problem for cashiers is that, with numerous major brand name companies issuing such checks (Visa, MasterCard, American Express, Diners Club and Thomas Cook, to name a few) 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. Generally speaking, it is beyond the scope of what can be thought of as reasonable for one person to remember all of these details.

Treasury Checks

Sixty-nine thousand U.S. Treasury checks were forged or altered in fiscal year 2008. The losses associated with these counterfeited Treasury checks were approximately $64.9 million dollars.[3] This level of annual loss was not uncommon, and follows a long-term trend dating back at least 60 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 depositories had been lost, forged or stolen. This fund still exists today.

[3]http://www.fms.treas.gov/checkclaims/questions.html#16

Personal Checks

Personal checks are a forger's playground.

The fastest growing financial crimes in America today are check fraud and identity theft. The Nilson Report estimates check fraud losses to be about $20 billion a year. The American Bankers Association (ABA) has stated check fraud is growing 25 percent per year. Check fraud gangs are hardworking and creative. They constantly try new 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 share the loss with the depositor.

The 2009 ABA Deposit Account Fraud Survey, which collects baseline information on check and electronic payment fraud losses, estimated that industry check-related losses amounted to $1.024 billion in 2008, up slightly from the $969 million in 2006 and marking the first time within the ABA's survey that check-related losses surpassed one billion dollars

FinCEN's SAR Activity Review, By the Numbers, published in January 2010, concluded that reported instances of check fraud increased 19% in the first six months of 2009, compared to the corresponding six-month reporting period in 2008. SARs listing counterfeit check increased 36%, compared to the corresponding six-month period in 2008.

In a 2008 interview, Frank Abagnale, the "celebrity" criminal forger whose life story was featured in the movie "Catch Me if You Can", was quoted as saying

"I simply don't understand why the US still uses checks, if it's costing $20 billion a year. That's something like $200 per household per year - more than enough money to make it worthwhile switching, as all of Europe has done, to electronic payments. If there aren't any checks, there isn't any check forgery - and when was the last time you saw a check in Europe? They basically don't exist, certainly not personal checks."
Read more: *http://www.portfolio.com/views/blogs/market-movers/2008/05/20/check-forgery-datapoint-of-the-day/#ixzz1JY9sFp21*

Store Coupons and Store Currency

Coupon fraud is the illegal reproduction of commercially issued discount coupons or store-promotion currency. 2009 saw a greater than 400% increase in incidences of this type of fraud over the previous year. The cost of these counterfeits has easily been in the tens of millions of dollars, according to a survey of 24 major consumer-products manufacturers. One consumer-product manufacturer estimates its losses to counterfeit coupons at more than $3 million a year. Return Receipt fraud is now one of the leading causes of fraud loss in the retail industry. According to the National Retail Federation's annual Return Fraud Survey, the industry lost an estimated $2.7 billion in return fraud during the 2009 holiday season, and an estimated $9.6 billion for the year.

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. Those that offer cents off can range from 50 cents to as high as $11.99.

Credit Cards, Gift Cards and Stored Value Cards

It should be news to nobody that credit card fraud has become an insidious problem. The cost of credit card fraud in 2006 was 7 cents per 100 dollars worth of transactions.[4] Because of the enormously-high volume of transactions this translates to billions of dollars per year. The U.S. Federal Trade Commission reported a 28% increase in such losses year-over-year from 2007 to 2008.[5]

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 under another's identity. Following is a brief summary of the more common techniques for obtaining fraudulent credit card data.

Card not present transaction

The mail and the Internet are major routes for fraud against merchants who sell and ship products, and affects legitimate mail-order and Internet merchants. If the card is not physically present the merchant must rely on the holder (or someone purporting to be so) presenting the information indirectly, whether by mail, telephone or over the Internet. While there are safeguards to this, it is still more risky than presenting in person, and indeed card issuers tend to charge a greater transaction rate for CNP, because of the greater risk.

It is difficult for a merchant to verify that the actual cardholder is indeed authorizing the purchase. Shipping companies can guarantee delivery to a location, but they are not required to check identification and they are usually not involved in processing payments for the merchandise. A common recent preventive measure for merchants is to allow shipment only to an address approved by the cardholder, and merchant banking systems offer simple methods of verifying this information.

[4]"Credit Card Issuer Fraud Management, Report Highlights, December 2008". Mercator Advisory Group. 2008.
[5]"Consumer Sentinal Network Data Book: January - December 2008" (PDF). Federal Trade Commission. February 26, 2009.

Identity theft

Identity theft-related credit card fraud is generally divided into two primary categories, application fraud and account takeover.

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 genuine cardholder, and asking for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent.
Skimming

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant. The thief can procure a victim's credit card number using basic methods such as photocopying receipts or more advanced methods 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 the victim's credit card out of their immediate view. The thief may also use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Instances of skimming have been reported where the perpetrator has put a device over the card slot of an ATM which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera to read the user's PIN at the same time. Another technique used is a keypad overlay that matches up with the buttons of the legitimate keypad below it and presses them when operated, but records or transmits the keylog of the PIN entered by wireless. The device or group of devices illicitly installed on an ATM are also colloquially known as a "skimmer".

Carding

Carding is a term used for a process to verify the validity of stolen card data. The thief presents the card information on a website that has real-time transaction processing. If the card is processed successfully, the thief knows that the card is still good. The specific item purchased is immaterial, and the thief does not need to purchase an actual product; a Web site subscription or charitable donation would be 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. A website known to be susceptible to carding is known as a cardable website.

In the past, carders used computer programs called "generators" to produce a sequence of credit card numbers, and then test them to see which were valid accounts. Nowadays, carding is more typically used to verify credit card data obtained directly from the victims by skimming or phishing.

A set of credit card details that has been verified in this way is known in fraud circles as a phish. A carder will typically sell data files of the phish to other individuals who will carry out the actual fraud

BIN attack.

Credit cards are produced in BIN ranges. Where an issuer does not use random generation of the card number, it is possible for an attacker to obtain one good card number and generate valid card numbers by changing the last four numbers using a generator. The expiry date of these cards would most likely be the same as the good card.

Counterfeit Fraud Losses

Statistics regarding counterfeit fraud losses are alarming.

As stated in a previous section of this paper, counterfeit currency has been growing at an alarming rate. The U.S. Treasury released a report in 2009 stating that there are approximately $400 million in counterfeit currency circulating in the U.S. We believe this figure to be grossly understated, since the Secret Service reports having confiscated $103M in 2008 and $182M in 2009. The Secret Service also reports their domestic seizure rates to be at or below 20%, thus implying that actual counterfeit currency in circulation, domestically, in 2009 may have been closer to $900 Million.

The American Bankers Association reported that there are $12.2 billion in losses due to check fraud every year.

A research report by the Mercator Group in 2008 found that losses due to credit card fraud were 7 cents per 100 dollars' worth of transactions.[6] Due to the high volume of transactions this translates to billions of dollars per year.

The Multiplier Effect

In 2010, Lexis–Nexis released their annual "True Cost of Fraud Study". One of the key takeaways from this report was the stunning fact that: "For every $100 of fraud, total losses equal $310".

[6]"Credit Card Issuer Fraud Management, Report Highlights, December, 2008". Mercator Advisory Group. 2008

In other words, a company that accepts a "hard-cost" loss of $1000 due to a counterfeit item may actually end up incurring an additional $2000 in "soft costs" before the case is closed. Soft costs include such things as: accounting audits, LP investigations, filing Suspicious Activity Reports with the FBI, filing Currency Transaction Reports, interviewing employees, legal consultation, loss recovery (pursuit of lost funds), fees, etc.

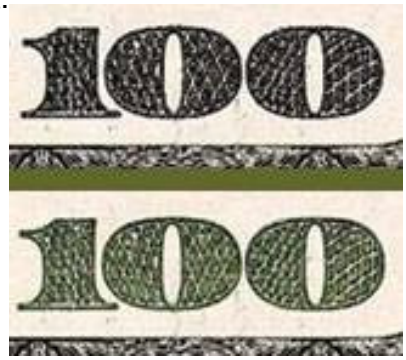
Detecting Counterfeit Instruments

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

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

Visible / Physical Document Inspection

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



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

Color Shifting Ink

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

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

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

Holographic Images

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

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

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

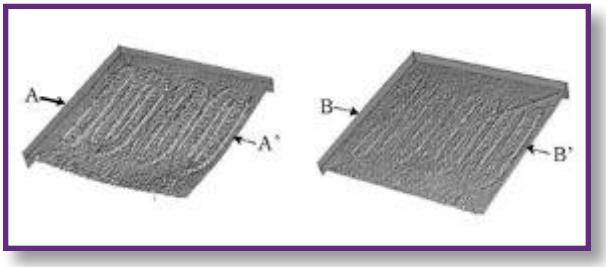
Thermal Ink

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

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

Intaglio Printing

Intaglio printing is really the master overt defense for "printed" document security. Intaglio is a printing technique which utilizes intricately carved printing plates and extremely heavy printing presses to physically alter the surface of the paper that is printed on. Very fine-details in the carved printing plates will cause ink to be forced into the fibers of the paper, creating a distinctive "raised feel" to the paper.



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

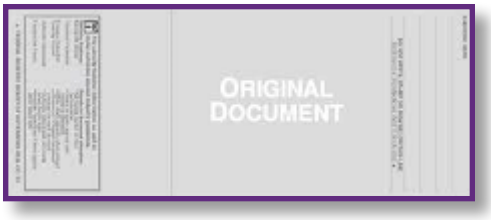
As a result of using intaglio technique, printers are able to produce very fine-detail in their printing. Consider this image of the US $100 bill. The very fine-line details both on Benjamin Franklin's face, and in the surrounding oval are produced at a level of resolution that an ink-jet or laser jet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

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

Watermarks

Watermarks come in two general categories "genuine" or "artificial". Contrary to what these terms may mean in the context of a discussion on the topic of this paper, both these types of watermark are "real". The difference between a genuine and artificial watermark is how the watermark is created. In the case of a genuine watermark, a pattern or image is carved into mold, and the mold is used to "emboss" the watermark into the paper. That is, physically stamped in a technique that produces both a visible image and a sub-surface-level raised depiction of the image.

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



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

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

Covert Feature Detection

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

- Microprinting
- InfraRed
- Magnetic
- UltraViolet

Microprinting

As the name suggests, microprinting is a technique in which extraordinarily fine detailed printing is performed on a document. In the case of US currency notes, microprinted features are typically words printed in characters too small for the naked eye to see. As the example to the right shows, the newest design US $50 banknote contains several different areas on the note where different microprinted security features can be found.

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

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

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

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

InfraRed Printing

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

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

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

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

Magnetic Character Printing

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

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

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

Ultraviolet Inks

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

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

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

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

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

Scientific Analysis

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

- Pattern Matching
- Machine readable zones/Data matching

These two concepts are based upon different authentication strategies.

Pattern Matching

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

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

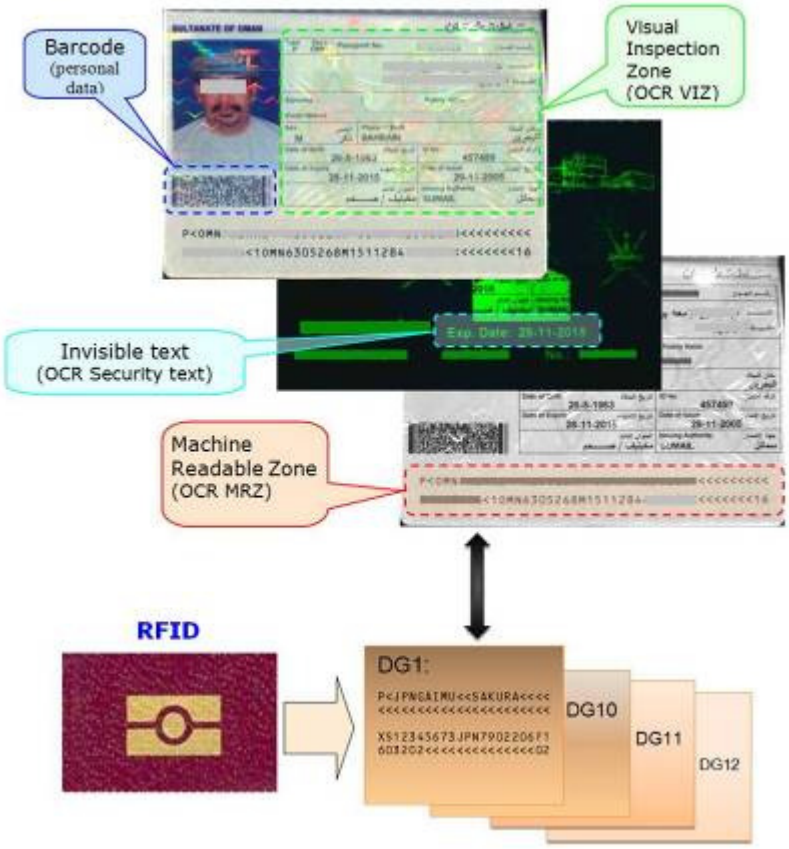
To verify the pattern of any given document, an intelligent library (database) is built that provides for a set of templates against which any document presented can be compared. Hardware devices then capture images of the document being tested, and those images are run through the database to identify,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

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

Data Compare

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

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



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

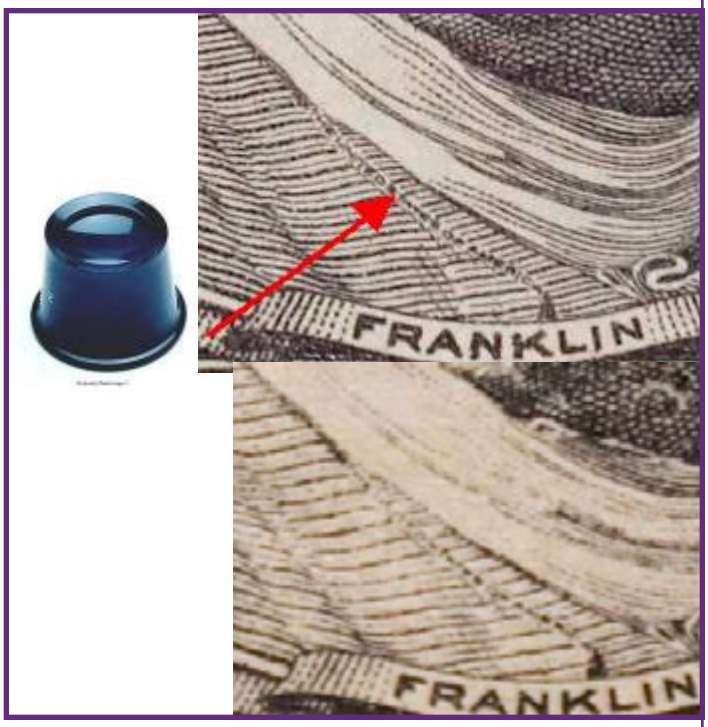
After identifying the document type, "data compare" devices will first look to see whether all of the expected forms of data are available. Then, it will proceed to pull all of the available data and put it into a table so that the field content can be compared. Each of the above listed methods of storing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

Tools for Counterfeit Document Detection

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

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

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



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

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

Visible Review Aids

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

Magnifier/Jeweler's Loop

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

Because microprinting requires advanced off-set printing techniques, many counterfeit documents either do not contain any microprinting, or the quality of the printing is very poor and can be easily identified when viewed under magnification. In fact, the magnifier can be used to view

any fine-line details that occur in higher-level off-set or intaglio printed documents. As the images to the right show, the genuine document (top) contains clear-to-see printing in the collar and very fine-detailed lines elsewhere, while the digitally reproduced copy (below) is unable to mimic these features accurately.

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

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

Infra-Red Viewers

As discussed in the previous section when we explored the concept of infra-red security printing as a security technique, there are products available that allow a transaction-counter employee to view documents under infra-red light. Devices such as this one, pictured to the right, use IR light sources to activate the IR inks, and then an imaging display screen to render the IR ink imagery into black & white.

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

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

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

Magnetic Ink Detector Devices

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

The concept of using this feature – e.g. – magnetic ink – as a technique to validate currency at the point of sale by a cashier or a teller is based on the belief that, if a device can detect the presence of magnetic ink on a banknote, then the bill must be genuine. Accordingly, numerous manufacturers have produced low-cost (as low as $5.95, in some cases) tools that can be manually traced across the surface of a banknote, and when it detects a magnetic field, it will indicate, with a red light, or a tone or some other method to notify the user that it found a magnetic feature.

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

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

More problematic are the range of devices purporting to be “advanced” bill detectors, which do nothing more than give a “red” or “green” light to indicate whether a bill is false or genuine. These devices are, in fact, doing the same thing as the little $6 device pictured above, but they cost the user from $99 - $149 dollars! Models currently marketed in the U.S., such as the D450 and the CashScan are guilty of this deception.

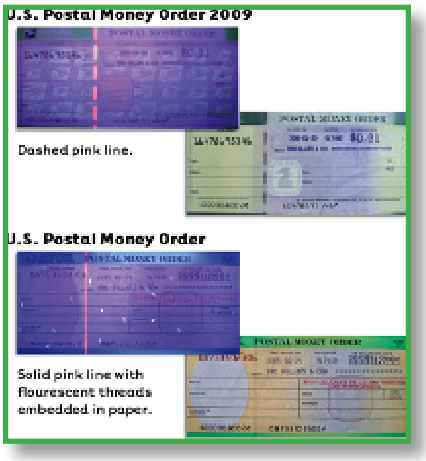
UV Lights

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

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

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

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



CON’s – Disadvantages of UV lights are similar to those that pertain to the other visible verification techniques, namely, that it requires a human being to interact with the document and make a logical decision, i.e. – “Yes, I see the proper UV security feature”. Many organizations do not wish to devolve this type of decision-making to the

transaction level employee. Lack of proper training can produce confusion and inaccurate results. If an employee has not been told what to look for, or hasn't been provided with proper materials for reference, they could easily decide that they have received a genuine item when, in fact, it is counterfeit. One such example of this type of circumstance might arise in the case of a "washed $5 bill". This banknote – a counterfeit note printed on top of a genuine $5 bill – will show the "blue" $5 security feature when placed under a UV light. However, if it is a counterfeit $100 bill, this blue feature should be a dead giveaway, since the proper security feature for the $100 bill is "red". Improper training may lead to this type of event. A final potential issue with UV security features is that, while difficult to counterfeit, they are by no means impossible to reproduce, thus, it is possible that counterfeit documents can make it past this level of scrutiny.

Advanced Analysis Devices

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

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

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

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

Machine Readable Character Reading Devices

Currency Detection

The marketplace has numerous devices designed to read Machine Readable features on currency notes to identify them as genuine. Buyers should be cautious before buying such devices that rely

on only one type of MRC read. For example, those machines that utilize only magnetic ink, or look only at IR printing as a means of authentication. Instead, care should be taken to choose devices that test for multiple features and then cross-check the results to ensure that authentication will be reliable. Devices that read IR, Magnetic, UV, intaglio and other features in combination will be much more difficult for counterfeiters to defeat.

Identity Document Detection

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

Data Compare Devices

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

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

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

The results of this test will enable the software to determine a level of probability that the document is genuine.

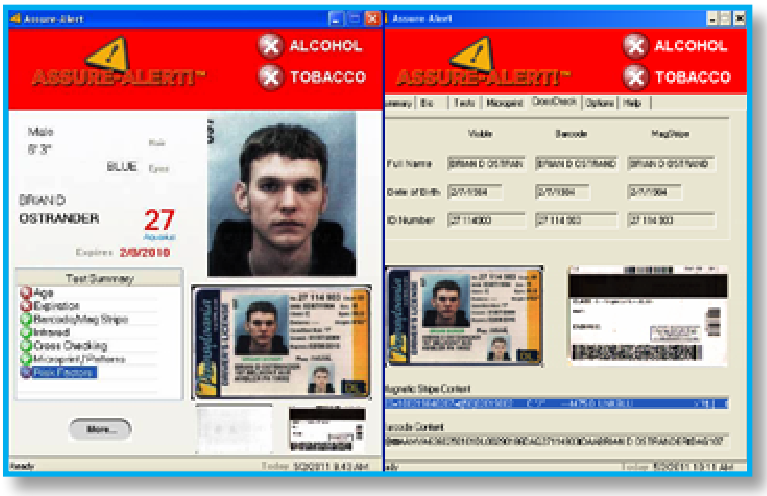
Pattern Matching Devices

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

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

Hybrid Pattern Match/Data Compare Devices

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



Another device that fits this final category description is L1's B-5000 document authenticator. L1 Identity Solutions is the manufacturer of choice for the design and production of identity documents for the US government and 46 US state driver licenses. They also manufacturer a very large number of international ID documents. The B5000 is able to "read" ID1 documents, and passports and other global ID formats. Because L1 manufactures many of these documents, their pattern matching "library" is extremely robust.

The B5000 unit is, in fact, a high-resolution camera which has built-in light sources that allow it to capture document images in IR, UV and white-light. These images are compared to its document library and high-confidence document authentication can be performed. This machine is also equipped with RFID and smart-chip readers to capture the information stored on them. The B5000 is capable of reading MRZ "zones" standard to ICAO document formats, and is B900 ink-capable. It can read mag-strip and bar-code data, and is also capable of conducting OCR reads of the printed information.

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

Multi-Layered Approach to Fraud Detection

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

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

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

MULTIPLE POINTS OF VULNERABILITY

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

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

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

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

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

The "Displacement Effect"

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

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.

Conclusions

The statistical evidence is quite clear: counterfeiting of valuable documents is on the rise. Whether one looks at 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 resulted in a clear and alarming rate of growth in the incidences of circulated forgeries for all document types.

Losses experienced as the result of these crimes by commercial organizations are astounding. Close to a trillion dollars, annually, from all types of counterfeit fraud, globally. When the additional "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 substantial.

Organizations not only experience 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 some form of 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.

In response to the long-term issues associated with counterfeit fraud, specialty companies have responded with products that enable organizations to conduct document review with the goal of aiding the user in confirming that one or more of the security features are present. More advanced equipment will not just verify the existence of the security feature, but will also validate that it is an accurate feature, containing the proper attributes, and thus, can provide a higher-level confidence assessment as to whether the document is genuine or not. At the "high-end" of the document authentication scale are those products that are able to read encoded information, and compare the design and layout of specific features in the document to provide a definitive answer, including a probability score, as to whether or not the document is authentic.

As to which of these products an organization should use – the best answer requires an analysis of the organization's exposure to different types of fraud during the different transaction-types conducted by that organization 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.