Defeating Fraud Through the Use of New Security Printing Features

Thomas M. Plutchak
NexPress Solutions, Inc.
Rochester, New York, USA

Abstract

Fraud takes many forms and is a large and growing problem around the world. Historically bank checks have been a favorite means for fraud, but fraud also takes many other forms including: counterfeit products (brand name clothing, inkjet cartridges, perfume, etc.), counterfeit or altered documents (passports, drivers licenses, birth certificates, stock certificates, car titles, etc.), and counterfeit event tickets (ball games, concerts, etc.). This paper will review traditional and new printing technologies which may be used to thwart all of these forms of fraud. These technologies are best used in various combinations and may be used either overtly or covertly. Particular emphasis will be placed on variable data microprinting as a new and powerful fraud prevention tool.

The Fraud Problem

Fraud takes many forms and is a large and growing problem around the world. Occupational related fraud losses in the United States alone have been estimated by the Association of Certified Fraud Examiners to be as much as $660 billion in 2004. While much of this fraud was in forms such as larceny and fraudulent accounting and financial statements (think Enron, Worldcom, and others), more than 20% of this fraud involved checks.

Other estimates by various organizations of the cost of check fraud alone in the United States vary widely ($4 billion to $24 billion per year), but all agree that the problem is very large and growing.

U.S. Customs and Border Protection now estimates that product counterfeiting costs the U.S. economy more than $250 billion per year.

This paper will talk about fraud prevention in the context of bank checks, but the security features discussed are equally applicable to the prevention of many other types of fraud, e.g. counterfeit product labeling, counterfeit or altered birth certificates or passports, and counterfeit event tickets.

Traditional Methods Used to Thwart Check Fraud

Check fraud can be categorized into three types:

Forgery – falsifying the signature on an otherwise legitimate document.

Counterfeiting – creating or reproducing a check. (Copying is subset of counterfeiting.)

Alteration – changing the payee and/or amount on a check. (Checks printed using toner are considered to be especially susceptible to alteration.)

This paper will introduce variable data microprinting as a powerful new feature capable of defeating fraud by both **counterfeiting** and **alteration**.

Different types of countermeasures can be used to defeat fraud. The ANSI publication X9/TG-8-2002, Check Security Guideline, lists features that can be used to defeat fraud by counterfeiting and by alteration and rates the effectiveness of each feature on a scale of 0 to 10 with 10 being the most effective. Most of these features are effective for defeating either counterfeiting or alteration, not both.

Fifty features aimed at defeating **counterfeiting** are listed with an average effectiveness of 6.8. Examples of the features listed are fine line printing, watermarks, pastel color fades, thermochromic inks, pantographs, and microprinting.

The publication lists far fewer features for defeating **alteration** (23) and rates them as being far less effective on average (4.2). Examples of features listed are invisible UV fluorescent ink, solvent sensitive inks, water sensitive inks, "toner lock" coatings, and adhesion promoting varnish.

Fraud prevention experts recommend that checks contain a minimum of three security features to protect against fraud. And these security features must collectively protect against fraud by both counterfeiting and alteration. Variable data microprinting will be shown to provide protection against counterfeiting, like traditional microprinting, while also adding powerful protection against fraud by alteration.

Traditional Microprinting

Traditional microprinting is found on checks, currency, and many other documents. It is small printing that appears to the unaided eye as a solid line. Low power magnification renders the printing readable. It is recommended that microprinting be smaller than about 0.7 point size, but examples between 0.6 and 1.0 point size are common (characters ~0.008 to 0.014 inches high).

Security features can be either overt or covert. The Check Security Guideline lists microprinting as a covert feature, but it is commonly used as an overt feature on checks. The signature line on checks is often actually a line of microprint text and a stylized MP symbol is used to indicate the presence of microprinting.

Traditional microprinting is done using traditional printing methods, such as lithography, and is static, i.e. it is exactly the same on each check or other document.

Since microprinting requires very high quality printing and is generally lost if a check is copied, it is considered to offer fair protection against counterfeiting. The Check Security Guide rates its effectiveness at 8.

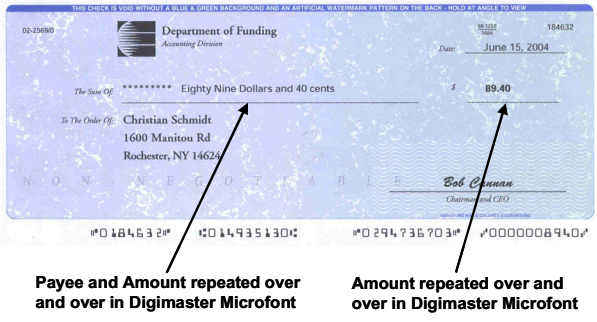
Traditional microprinting, however, offers no protection against fraud by alteration.

Variable Data Microprinting

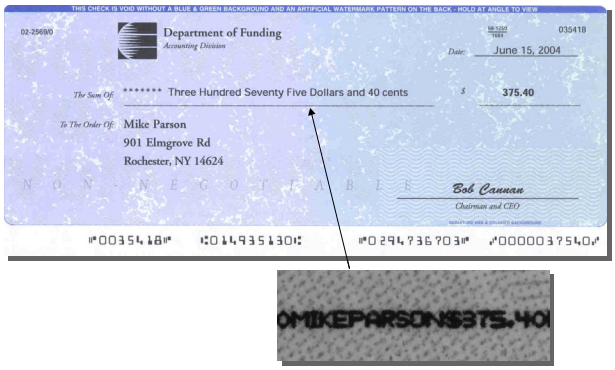
New printing systems such as the Kodak Digimaster digital production systems and the NexPress 2100 digital production color press offer a level and consistency of image quality that was previously unavailable. This level of image quality combined with specially optimized small fonts now enables variable data microprinting as a new security feature. Variable data microprinting defeats fraud through both counterfeiting and alteration. Key variable data drawn from data on the document itself can now be printed using microprinting. This microprinting, like traditional static microprinting, is difficult to produce and is generally lost if the document is copied. In addition, the key variable data that is printed using microprinting is difficult or impossible to alter. Like traditional micro-printing, variable data microprinting is inherently a covert feature but it can be made overt by alerting the observer to its presence.

Some Examples and Applications

A good example of the use of microprinting is illustrated in the figures below.



In this example the name of the payee and the amount of the check are printed over and over again using a microfont under the written amount of the check. The amount of the check is printed over and over again under the courtesy amount. This variable data microprinting appears to be lines to the unaided eye but is rendered readable with low level magnification.



In this application variable data microprinting adds a powerful new level of security since the microprinting is difficult or impossible to either copy or alter. Perhaps best of all, variable data microprinting is a security feature that can be added at no cost if the documents are printed on a printing system that is capable of printing a microfont that is consistently readable. Many other security features are expensive to add, e.g. thermochromic and UV fluorescent inks.

There are many other applications for which variable data microprinting can add a new and powerful level of security:

Insurance documents
Event tickets
Printed voting ballots
Car titles
Birth certificates
Passports
Stock certificates
Packaging for high value products
Warranty documents

Biography

Tom Plutchak received a B.S. in physics from Michigan Technological University in 1969. Since then he has had 35 years of experience in researching, developing, and commercializing printing technologies for Eastman Kodak, Heidelberg, and NexPress Solutions. He has held numerous supervisory positions with responsibilities for fuser technology, novel color imaging systems, photoconductor technology, and strategic planning. Most recently he was the program manager responsible for the commercialization of the Kodak Digimaster series of MICR printers.