
# PROTECTING YOUR ASSETS FROM THE GROWING PROBLEM OF DOCUMENT FRAUD

wise

Jeff Prettyman
Executive Vice President
Wise

APPVION

Mike Caffrey
Security Business Development Manager
Appvion

# In the Crosshairs

## Protecting your assets from the growing problem of document fraud

Inasmuch as digital technology has opened vast new horizons for communications, education, economics, and business, it has also created potent opportunity for criminal fraud. Inexpensive computers, scanners and printers now make it easy for anyone to falsify valuable documents. In the same sense, the connectivity of the Internet has fostered unprecedented worldwide commerce, but also serves as a venue for criminal fraud. As recently reported:

> Fraud is ubiquitous; it does not discriminate in its occurrence. And while anti-fraud controls can effectively reduce the likelihood and potential impact of fraud, the truth is that no entity is immune to this threat.[1]

Among financial instruments, checks remain a favored target of criminals. A 2013 study[2] reported that 92% of organizations still use checks when paying at least some of their major vendors/suppliers, and that the average company makes 43% of its payments to major suppliers by check. A 2014 survey reported that 70% of B2B payments are still made via check.[3]

### A Very Serious Threat

In 2012, checks (consumer and business) had the highest average value of unauthorized transactions. The average unauthorized check transaction was valued at $1221, as compared to ACH at $730, ATM withdrawals at $217, general purpose credit cards at $138, and general purpose debit cards at $105.[4]

> While the exciting and glamorous fraud topics today involve wire fraud, account takeovers, ID theft, and skimming, the results of the Association for Financial Professionals' annual corporate fraud survey remind us that the most fraud vulnerable instrument available today is the paper check.
>
> -Richard Oliver, Atlanta Federal Reserve Bank, May 2011

The Information Security Media Group noted 2013 that 52% of organizations have experienced check fraud in the past year.[5] In 2014, a different survey [6] concurred that checks remain the payment type most vulnerable to fraud attacks, and that 82% of organizations affected by payment fraud report that checks were targeted. And, among organizations suffering a loss due to payments fraud, the typical amount was $23,100.[6]

Unfortunately, check fraud is just one part of the problem. Other value-bearing documents such as secured notes, stocks, bonds, letters of credit, and coupons are also vulnerable. In addition, documents establishing personal identity, ownership or origin can be fraudulently used in ways that ultimately cause a monetary loss for some one or some organization. There are, however, relatively simple and straightforward strategies to thwart document fraud. First we'll focus on checks, the most frequent target.

### Protecting Your Business from Check Fraud

Estimates place the cost of check fraud alone to American businesses and banks at approximately $50 billion a year[7]. A staggering amount, but check fraud is so popular because it's so easy. Anyone with a personal computer, scanner and inkjet printer can create fraudulent checks that would pass even expert inspection. With access to only basic account information, fraud criminals can easily and quickly generate hundreds of counterfeit or forged checks.

### Begin By Looking Inside

The starting place for any fraud prevention program is inside the organization. Carefully review your check writing procedures. It's best to limit the number of people authorized to issue checks — regrettably, employees are often the

perpetrators in business check fraud schemes. Placing dollar limits on check authorizations can also help. Reconciling your accounts on a timely basis will quickly bring discrepancies to light. Finally, making sure that all employees know the company follows strict audit and accounting procedures will discourage temptation.

### Secure Your Checks

Next, it's important to use checks that include a variety of security features designed to combat specific types of fraud schemes. The most common types of check fraud include:


- **Counterfeiting**: creating a fake check (e.g., via desktop publishing).
- **Forging**: signing a check without authorization.
- **Paperhanging**: writing checks on a closed account.
- **Washing**: using chemicals to remove ink from a check to change the payee and/or amount.
- **Scraping**: using abrasives to remove printed or written information (e.g., payee or amount) which is then replaced with fraudulent information.
- **Lifting**: using tapes, razor blades or fine knives to remove or cut-and-paste information from one part of a check to another.
- **Raising**: Changing the dollar amount by adding a digit ($50.00 to $500.00).

The most effective ways to deter fraud is to use checks with specific features to foil these methods. Fraud criminals tend to focus on the easiest and most vulnerable targets. All you have to do is make your checks more difficult attack and the criminals will seek easier marks.

### It's Not Just a Check Problem

While it is evident that a significant amount of financial fraud exists, the risk is not limited to this area. Fraud also occurs in other areas such as the medical and higher education fields. Counterfeit prescription pads, altered prescription pads, forged credentials, falsified insurance claims, and doctored insurance cards are just a few of the techniques and schemes used to commit fraud. These deceptions almost always involve fraudulent documents.

A 2011 White House study indicated that the misuse of prescription drugs continues to rise rapidly. Some experts report that it is the nation's fasting growing drug problem.[8] That same study noted that illicit drug use costs the US economy in excess of $193 billion annually.

Another large fraudulent document issue in the medical field is falsified insurance claims. The Cornell University Law School recently reported that 10 cents of each dollar spent on healthcare goes to paying fraudulent healthcare claims.[9]

In addition, the higher education field is also not immune to altered documents that defraud the public and educational institutions. Documents that educators use to certify graduation, recommend or reference candidates, or qualify for grants and scholarships all carry unique and significant value. These documents are also the targets of criminals perpetrating fraud.

In a presentation before the House of Representatives one international "diploma mill" sold over 450,000 counterfeit diplomas and grade transcripts. The gross amount of the revenues generated from these documents was estimated at $435 million.[10]

A 2013 report estimated that 50,000 fake PhD degrees are sold each year. By comparison, between 40,000 to 45,000 PhD degrees are awarded by accredited schools in the United States each year.[11] In a related application to transcript

fraud, the Sheriff's office of Palm Beach, FL, reported that more than 30 applicants for nursing licenses used forged or altered transcripts.[12] Obviously the risk to us is not limited to financial applications.

### Security Strategies

There are two ways to incorporate fraud protection into your secure documents themselves. The first is within the paper itself and how it is manufactured. The second method uses a variety of printed features that defy fraud methods. By combining these two, you can create documents that are so difficult to attack that criminals will go elsewhere.

### In-Paper Security


In-paper features are built into the paper during manufacture. Duplicating these are often beyond the capabilities of all but the most skilled criminals. A true watermark is a good example. Created within the fiber structure of the paper during the papermaking process, true watermarks are exceptionally difficult to reproduce. While among the more costly security features, a true watermark is also among the most proven fraud deterrents. There are also a number of other very effective in-paper features including:

- **Artificial watermarks** — this technique creates a watermark-like image in the reflectivity of the paper.
- **Indicator stains** — special coatings that permanently change color when exposed to the solvents used in check washing.
- **Fibers** — small colored strands in the paper structure that can either be visible to the naked eye, or made with materials only visible under UV illumination.
- **Tamper-proof patterns** — subtle repeated markings coated on the document that reveal if the surface has been scraped or information has been lifted.
- **Toner adhesion** — coatings that create a stronger, tamper-resistant bond between printing toner and the paper surface.

### On-Paper Security

On-paper features, added after the paper has been manufactured, offer enhanced protection. They also provide a means of easily customizing your security system. A good example is micro-printing, which yields type so small it appears to be a straight line to the eye. Yet, under magnification, it is readable. Micro-printing is beyond the resolution of most digital printers, and therefore very difficult to reproduce. There are many other on-paper features such as:

- **Abrasion-reactive inks** — used for the printed information on the check, but changes color if subjected to abrasion.
- **Thermochromic inks** — used for emblems or graphic marks on checks or other documents, changes color or disappears when touched by the warmth of your finger.
- **Invisible inks** — create printing or patterns that are invisible under normal light, but readily visible under infra-red or ultra-violet (black) light.
- **Metameric inks** — inks that change colors in response to the direction from which illumination comes.
- **Void pantographs** — patterns or warning notices that are barely visible under normal light, but appear boldly when photocopied.
- **Holograms** — stickers with unique three-dimensional optical effects.

Many of the in-paper features mentioned above are available without special order, and therefore more economical than a true watermark, for example. These security papers are available through reputable sources, but there's a need for caution with regard to how such papers are stored and distributed. A stock with strong in-paper features will offer little real protection if the chain-of-custody is not adequately secure and fraud criminals can buy the stock as easily as anyone else.

The same holds for stocks with on-paper features. Some suppliers offer stocks with on-paper features already added. These can be further augmented with on-paper features added by a qualified and capable printer. By combining a comprehensive blend of these features, businesses or organizations can readily create an individual, customized paper with exceptional security.

**Don't Forget Users**

It is also important to ensure that people authorized to handle or negotiate your checks (or other financial instrument) are aware of the security features the paper offers. Some of these features, such as indicator stains, easily reveal problems. Other, more subtle features are only effective if people know to look for them.

Finally, be constantly vigilant. Assume that fraud criminals will be always be looking for weaknesses in your defenses. The best strategy is a strong preventive position. First, ensure your internal workings are secure. Then analyze the risks you face and develop an appropriate, cost-effective response. By working with your paper supplier and check printing resource, you can develop a plan that periodically alters the security features of your checks or other valuable documents.

That way, you'll keep your assets, financial health and image safe while keeping fraud criminals on their heels.

---

[1] 2014 Report to the Nations on Occupational Fraud and Abuse
[2] 2013 AFP Electronic Payments Survey
[3] Aite Group, "Remittance Details: When and How They Arrive for U.S.-Based Companies"
[4] 2013 Federal Reserve Payments Study
[5] Information Security Media Group (iSMG) 2013 Faces of Fraud Survey:
[6] 2014 AFP Payments Fraud and Control Survey findings show:
[7] https://www.city-bank.com/Pages/Business/Online-Services/Positive-Pay---Payee-Positive-Pay/
[8] 2011 Executive Office of the President of the United States
www.whitehouse.gov/administration/eop/cea/TheEconomicCaseforHealthCareReform
[9] Legal Information Institute at the Cornell University Law School www.law.cornell.edu/wex/healthcare_fraud
[10] Testimony of Allen Ezell before the U.S. House of Representatives, 9/23/2004
[11] "Does Your Doctor Have a Fake Degree?
The Billion Dollar Industry That Has Sold Over a Million Fake Diplomas", AlertNet, June 13, 2012
[12] The Palm Beach Post, December 19, 2010

## GEORGIA
555 McFarland/400 Drive
Alpharetta, GA 30004
Toll: 888-815-9473
P: 770-442-1060
F: 770-442-9849

## INDIANA
4301 Merchant Road
Ft. Wayne, IN 46818
Toll: 888-817-9473
P: 260-489-1561
F: 260-489-1955

## MAINE
33 McAlister Farm Road
Portland, ME 04103
Toll: 800-866-6560
P: 207-774-6560
F: 207-775-4728

## PENNSYLVANIA
150 Kriess Road
Butler, PA 16001
Toll: 888-813-9473
P: 724-789-9700
F: 724-789-9704

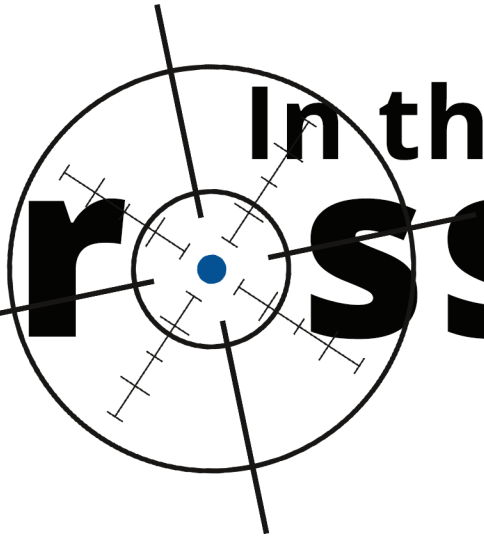
## SOUTH CAROLINA
118 Hurricane Creek Road
Piedmont, SC 29673
Toll: 800-445-2264
P: 864-845-5100
F: 864-845-5199

## CORPORATE
555 McFarland/400 Drive
Alpharetta, GA 30004
Toll: 888-815-9473
P: 770-442-1060
F: 770-751-3599

wise
print | technology | services

www.wbf.com • info@wbf.com

# In the Crosshairs



## Protecting your assets from the growing problem of document fraud

Written By:
Jeff Prettyman, Executive Vice President, Wise Business Forms
Mike Caffrey, Security Business Development Manager, Appvion