wise
forms | labels | digital

White Paper

Document Security:

Protecting Your Assets From Document Fraud

White Paper

Document Security: Protecting Your Assets From Document Fraud

Content

Introduction 2

Types of Check Fraud 3

It's Not Just a Check Problem 4-5

Stay Vigilant 6

Introduction

Even as digital technology has opened vast new horizons for everything from marketing to shopping to business, it has also created potent opportunities for criminal fraud. The same powerful computers, scanners, and printers that simplify and empower our daily lives also make it easy for anyone to falsify valuable documents.

Document fraud isn't just a concern for large companies. It is a considerable threat even to small and midsized ones. Smaller companies tend to have fewer protections and be easier targets.

Document Fraud Is Everywhere

When we think about document fraud, we often think about checks. It's true—checks remain a favored target of document criminals. However, they are not the only targets. According to USLegal, the top types of documents forged and altered include the following: [1]

- Checks and currency
- Bills of exchange and lading
- Promissory notes
- Money orders
- Titles and deeds
- Securities and bonds
- Court seals
- Corporate documents
- Documents used in identity theft

A variety of other everyday documents such as college transcripts, diplomas, and prescription pads are common targets of forgery and alteration, as well.

Check Fraud Remains Rampant

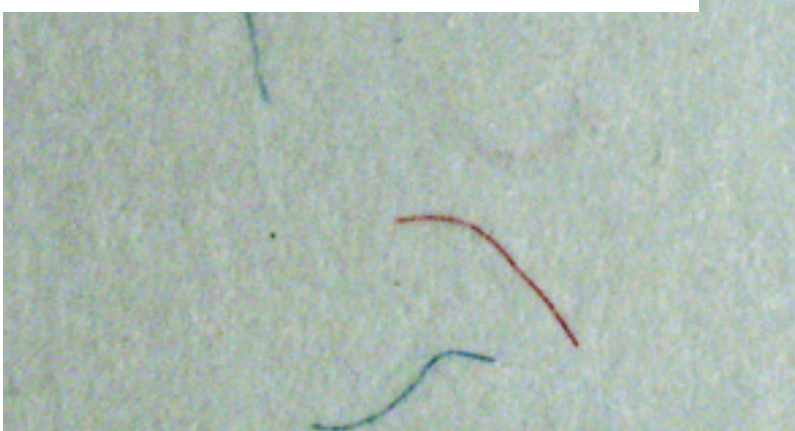
Check fraud remains the most common type of document fraud. According to the Association for Financial Professionals ("2021 AFP Payments Fraud and Control Survey"), 66% of respondents agree that, in spite of the decline in check usage, fraudulent checks remain one of their major concerns.

As the report notes,

> The rise in check fraud statistics continues as fraudsters become more advanced in their crimes . . . With a reported 500,000 check fraud scam victims in the U.S. each year, check fraud attempts increased to $15.1 billion in 2018—up from $8.5 billion in 2016—and accounted for 60% of attempted fraud against deposit accounts at U.S. banks. [2]

With the rise in digital commerce, this may be a surprise to some. Yet, while check use is down overall, checks remain an important part of our payment system. In fact, paper checks still account for 40% of B2B payments.[3] In the consumer marketplace, they account for 8.2% of all payments.[4] According to the Federal Trade Commission, 1.2 million fraudulent checks are processed through the banking system every day. Forged checks lead to about $10 billion in total annual losses.[5]

Even today, the potential for check fraud touches nearly everyone. According to the March 2020 PYMNTS playbook, 81% of businesses still pay other firms via paper checks, making it the most common B2B payment method.[6] In the consumer marketplace, nearly two-thirds (61%) of consumers used paper checks at least once over the past year. Check fraud remains 35% of all types of bank fraud.[7]



Types of Check Fraud

There are many different types of check fraud. In addition to fraudulent check presentations, such as check kiting and check floating, there are a variety of fraud tactics that involve the documents themselves. These include:

1. **Paperhanging:** Creating fake checks using easily obtainable materials such as blank check stock and a printer.

2. **Check forgery:** Altering an authentic check in some way, such as changing the payee or amount.

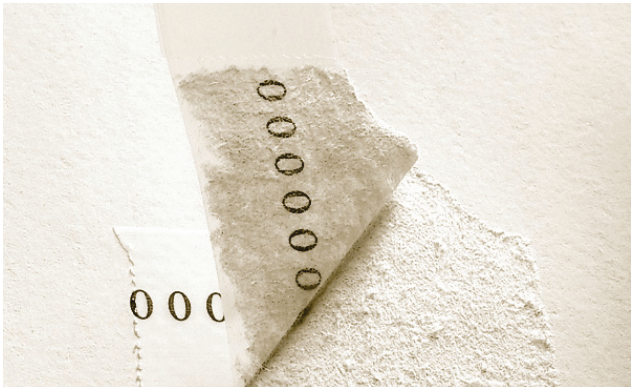
3. **Chemical alteration:** Using chemicals to change the appearance of a check. Examples include:

    - **Washing:** Using chemicals to remove ink from a check to change the payee and/or amount.
    - **Scraping:** Using abrasives to remove and replace printed/written information, such as payee or amount.
    - **Lifting:** Using tape, 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).

4. **Counterfeiting:** Creating fake checks that are identical to real ones, then presenting them for payment.

6. **Synthetic checks:** Combining elements from different types of payment instruments to create a new, fake check. For example, a thief might take the routing number from a legitimate check and combine it with the account number and personal information from a stolen credit card.

7. **Money order fraud:** This type of fraud occurs when someone counterfeits or alters a money order and presents it for payment.



[1] https://forgery.uslegal.com/types-of-forged-instruments.

[2] https://www.miteksystems.com/blog/what-is-check-fraud#

[3] https://www.pymnts.com/news/b2b- payments/2021/deep-dive-why-paper-checks-still-factor-into-b2b-firms-payment-optimization-plans/

[4] https://www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm

[5] https://www.consumer.ftc.gov/blog/2018/09/anatomy-fake-check-scam

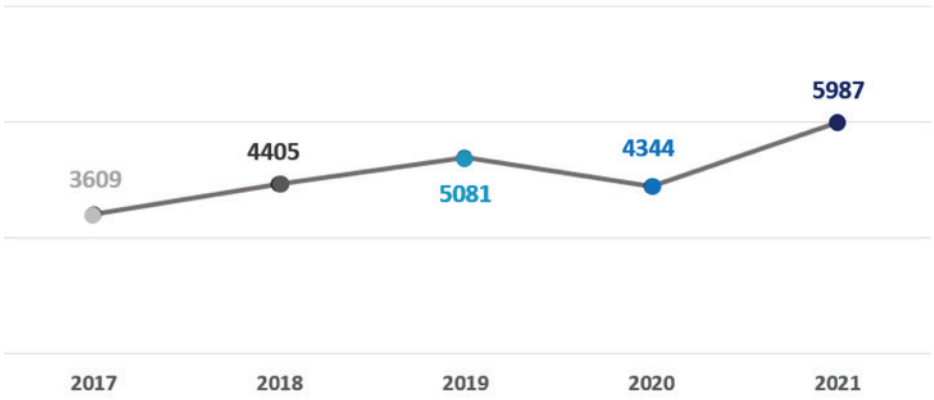
[6] https://www.pymnts.com/news/b2b-payments/2021/deep-dive-why-paper-checks-still-factor-into-b2b-firms-payment-optimization-plans/

[7] https://sqnbankingsystems.com/resources/articles/101-facts-about-check-fraud/

It's Not Just a Check Problem

Unfortunately, the risk of document fraud is not limited to checks. Counterfeit and altered prescription pads, forged credentials, falsified insurance claims, and doctored insurance cards are just a few other examples.

Take the healthcare industry. According to the Pharmaceutical Security Institute, there were 5,987 pharmaceutical crime incidents in CY 2021, including incidents of counterfeit prescription pads. This is up 38% from CY 2020. Falsified health insurance claims remain a huge problem, as well. According to the National Conference of State Legislatures, healthcare fraud costs insurers anywhere between $70 billion and $234 billion each year.



Source: https://www.psi-inc.org/incident-trends

Two Types of Fraud Protection

Considering the size of the problem, what can be done about it? The answer is to add document security features.

There are two ways to add security to your documents. The first is within the paper itself—in how the paper is manufactured. The second uses a variety of printed features on top of the paper. By combining these two, you can create documents that are incredibly difficult to attack.

1 . In-Paper Security

In-paper security features are built into the paper during manufacture. Duplicating these features is 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, true watermarks are 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.
- **Security 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.** Patterns that use subtle, repeated markings coated on the document to reveal whether the surface has been scraped or information has been lifted.
- **Improved toner adhesion.** The use of coatings to create a stronger, tamper-resistant bond between the printing toner and the paper surface.

1 . On-Paper Security

On-paper security features are added after the paper is manufactured and offer enhanced protection. Here are some common examples:

- **Micro-printing.** This technique yields type so small that it appears to be a straight line to the eye, yet under magnifi cation is readable. Micro-printing is beyond the resolution of most digital printers and is very diffi cult to reproduce.
- **Abrasion-reactive inks.** These inks are used for the printed information on the check and change color if subjected to abrasion.
- **Thermochromic inks.** These inks change color or disappear when touched by the warmth of your finger. They are commonly used for emblems or graphic marks on checks or other documents.
- **Invisible inks.** These inks create printing or patterns that are invisible under normal light but are readily visible under infrared or ultra-violet (black) light.
- **Metameric inks.** Inks that change colors in response to the direction from which illumination comes.
- **Void pantograph.** Patterns or warning notices that are barely visible under normal light but that appear boldly when photocopied.
- **Holograms.** Stickers with unique three-dimensional optical effects.
- **Printloc®**, an option that anchors the toner to the paper so that it cannot be lifted off.
- **Heat-sensitive symbols** (such as "Rx") that change colors when rubbed or heated.

By combining a comprehensive blend of both in-paper and on-paper features, businesses or organizations can readily create individual, customized documents with exceptional security.

How to Sell Document Security Features

Document security offers tremendous opportunities to sell into high-value and high-volume accounts. Among the companies you can target are those that offer tickets or coupons, medical or legal documents, financial documents, and transcripts, as well as any company with a finance department. How do you approach them? Start by researching the vertical market so you can come up with a plan.

Find answers to the following questions:

- Which documents are forged most often?
- How are they forged? (This will determine the security features needed to protect them.)
- When documents are forged, what is the financial loss that can occur?
- What are the safety and legal ramifications?
- Which specific document security features will protect against the types of alteration or forgery this vertical is experiencing?

Go in prepared. Ask if the company knows how much it is losing each year due to document forgery. If they don't know, have examples of the losses experienced by similar companies or to the industry as a whole. Be ready to present a problem/solution scenario that shows the value that document security brings.

Need help? Let us help you develop a strategy for building this profitable book of business.

Fraud Protection Starts Here

While adding document security features is a critical element, a comprehensive fraud prevention effort goes beyond in-paper and on-paper security features. It starts with the procedures, permissions, and workflow inside the customer's organization. As a distributor, you can add value to your client relationships by encouraging them to follow these industry-standard protocols:

- **Limit the number of people authorized to issue checks.** Employees are often the perpetrators in business check fraud schemes.
- **Place dollar limits on check authorizations.** Anything beyond a pre-set limit should require authorization.
- **Reconcile accounts on a timely basis.** This allows companies to catch discrepancies before they become larger problems.
- **Make sure that all employees know that the company follows strict audit and accounting procedures.** This will discourage temptation.
- **Add document security features to make checks more difficult, if not impossible, to counterfeit or alter.**

Fraud criminals tend to focus on the easiest and most vulnerable targets. Help your customers make their checks more difficult to attack, and the criminals will seek easier marks.

GEORGIA/ CORPORATE

555 McFarland 400 Drive
Alpharetta, GA 30004
T: 888-815-9473
F: 770-442-9849

INDIANA

4301 Merchant Road
Ft. Wayne, IN 46818
T: 888-817-9473
F: 260-489-1955

PENNSYLVANIA

150 Kriess Road
Butler, PA 16001
T: 888-813-9473
F: 724-789-9704

MAINE

33 McAlister Farm Road, Suite 100
Portland, ME 04103
T: 800-866-6560
F: 207-775-4728

SOUTH CAROLINA

601 Vanguard Road
Anderson, SC 29625
P: 888-817-7036
F: 864-226-8464

wise
forms | labels | digital

wbf.com • info@wbf.com