

[HOME](#) / FRAUD DETECTION AND PREVENTION

Loan Fraud Detection and Prevention with FTD Software (10 Important Visuals)

2 MAR 2021

[SAHIL KERKAR](#)

10 Important Visuals on [File Tampering Detection](#)

**Sahil Kerkar**
Data Scientist**Evan Zhang**
Senior Technical
Product Manager**Flaviu Andreescu**
Director of Engineering

One of the most difficult tasks for lenders is loan fraud detection, or more specifically, identifying [fraudulent loan applications](#). This challenge is pervasive in business, personal, and [mortgage lending](#), with the Covid-19 pandemic accelerating the problem when new processes were quickly introduced into the underwriting workflow. In this fast-paced and ever-changing environment, it is more crucial than ever for lenders to have the ability to adapt to evolving fraud tactics in order to further detect and prevent [loan fraud](#).

At Ocrolus, we process millions of financial documents each year and have studied the idiosyncrasies of potentially fraudulent activity. To aid lenders in [identifying suspicious activity](#) (and more importantly, the associated rise in loan defaults), Ocrolus has developed File Tampering Detection (FTD), a proprietary loan [fraud detection](#) technology that enhances our core service of automating financial document workflows. While document tampering itself is not proof of loan fraud, our analysis of thousands of loan outcomes has demonstrated that applications with tampered bank statements, [pay stubs](#), or tax documents perform significantly worse. With FTD technology, lenders now have the ability to identify red flags, prevent fraud and price loans more accurately.

How Can You Tell if a Document Has Been Tampered With?

It can be hard to tell when document tampering happens. The best way to [detect fraud](#) is to become familiar with what it most often looks like. Below are ten file tampering and loan fraud detection visuals that highlight fraud's pervasiveness in lending and detail Oculus' research on the relationship between altered documents and loan defaults.

An Alarming Increase in Document Fraud

With the world more digitized and transparent than ever before, fraudsters have come up with increasingly clever methods to get past electronic systems. In the annual Consumer Sentinel Network [report](#) published by the Federal Trade Commission, reports related to [financial fraud](#) and identity theft grew from 3.24M cases in 2019 to over 4.72M in 2020, an acceleration of an ongoing trend.

Further illuminating is the fact that identity theft is one of the fraud tactics rampant across institutions that produce documents used in lending decisions.

Top Types of Identity Theft

Rank	Theft Type	# of Reports
1	Government Documents/Benefits	406,375
2	Credit Card	393,207
3	Other	353,152
4	Loan/Lease	204,967
5	Employment/Tax	113,529
6	Utilities	99,539
7	Banks	89,476

An Overview of File Tampering Detection Technology

Oculus File Tampering Detection technology, also called document tampering detection, helps to [prevent any fraud](#) by analyzing documents to determine whether they have been edited after being originally produced by the issuing institution. By investigating every aspect of the document and its underlying data, document tampering detection can identify tampering undetectable by the human eye.

Of the 2.9 million documents Oculus received in 2020, approximately 1 percent showed evidence of file tampering.

Explaining Economic Changes with File Tampering Detection

Ocrolus document tampering technology captured an increase in file tampering over the summer related to the SBA's Payroll Protection Program (PPP), which offered loans that could be converted into grants for businesses affected by the pandemic. This data is consistent with the government's metrics on the widespread uptick in loan fraud during the program.

Interestingly, there were substantial differences in the rate of FTD by document type. Pay stub FTD was consistently lower (although nontrivial at around 1 percent), while W2 FTD was consistently higher (around 3 percent). Bank statement FTD tracked the overall aggregate trends in FTD rates across all document types. Lenders need to be aware that the types of documents they request can impact rates of suspicious activity, as certain documents may be easier or more important for applicants to manipulate than others. When these documents have been tampered with in any way, it's a sign that a borrower may be misrepresenting themselves, or attempting loan fraud.

On average, Ocrolus clients in 2020 submitted loan applications that had evidence on file tampering in 1.26 percent of cases. However, there was a lot of variation between lenders: some had close to zero evidence of document tampering, while the most extreme had an FTD rate of over 4 percent. It is crucial for lenders to understand where they fall on this spectrum to determine the prevalence of loan fraud in their pipeline.

Distribution of File Tampering Detection Rates Among Ocrolus Clients

As shown below, no type of lender is safe from file tampering. [Small business loans](#) (which included a substantial portion of PPP loans) had the highest FTD rate (2.1 percent) when compared to personal loans (1.1 percent) or residential mortgages (1.5 percent). However, even consumer loans still have significant FTD rates, demonstrating the value of file tampering detection technology across a wide variety of products.

Focusing just on [bank statements](#), there was variation in FTD rates by the type of organization that created the document. It may seem counterintuitive that statements issued by fintechs are tampered with most frequently, given the advanced technology often employed by these companies in their financial offerings. However, the rapid pace and volume of fintech decision-making may be attractive to fraudsters hoping to slip by unnoticed.

Another interesting discovery around loan fraud detection is that businesses in the transportation industry saw far more document tampering activity than those in other sectors.

With stay-at-home policies adopted across the country in 2020, research indicates that industries most impacted by the economic slowdown, including services and retail, had more incidents of potential fraud than stable industries like construction and finance.

Loan Fraud Detection Can Reduce Default and Improve Profitability

Ocrolus developed file tampering detection technology in conjunction with our lender partners. What has proven to be most revealing is retroactive analyses. We reviewed documents submitted during the application process for already funded loans, which allowed us to quantify the impact of document tampering on loan performance. After analyzing thousands of loans from multiple lenders, loans with one or more altered documents defaulted at a rate 18% more often than loans without FTD activity.

Furthermore, the percentage of principal that was not recovered was 1.17 times higher for FTD loans.

Finally, and most telling, the gross interest margin for loans with file tampering activity was 70 percent that of loans with no FTD activity.

On all of these performance metrics, document tampering detection has proven to be a statistically significant predictor of outcomes.

File Tampering Detection (FTD) is a powerful tool in identifying altered documentation and [preventing loan fraud](#). Loan applications containing tampered documents default more often and are less profitable than loans with verified documentation. Without advanced loan fraud detection technology, lenders are susceptible to mispricing loans, experiencing significant losses, and misclassifying fraud risk as credit risk.

Tags: [lending automation](#) | [file tampering detection](#)

SHARE THIS





AUTHOR

Sahil Kerkar

Sahil Kerkar is the Data Scientist here at Ocululus. Stay up to date on their industry insights.



VERTICAL SOLUTIONS

SMALL BUSINESS FUNDING

Cash flow analysis

Encore

MORTGAGE

Income calculations

Inspect

DEVELOPERS

API

Supported documents

COMPANY

Careers

Contact us

In the news

Legal

Partners

Referral program

Security & compliance

PLATFORM

Document understanding

Fraud detection

USE CASES

Auto finance

Consumer lending

Legal

Medicaid

Tax

Tenant screening

RESOURCES

AI Resource Center

Blogs

Customer stories

Videos

Whitepapers and eBooks

