Ocrolus

DETECT

Frequently Asked Questions (FAQs)

Ocrolus

Q: What is Detect?

A: Detect is a document fraud detection solution that empowers lenders to make quicker lending decisions and confidently process more loans. Detect was designed to signal to lenders when intentionally deceitful document tampering has occurred. Detect aims to provide the necessary level of context to help support decision making and streamline existing lending review workflows.

Fraud review processes are nuanced and unique to individual lenders; tolerance levels for document tampering also vary. Detect was not designed to make final determinations about borrowers or final lending decisions. Lenders should have a pre-established review process, workflow or set of best practices that outline the steps that should be taken when potential fraud is encountered and how to proceed with borrowers.

Q: How does Detect know a document has been tampered? What is being signaled ?

A: Detect leverages Ocrolus' sophisticated AI and machine learning capabilities, along with an extensive document dataset, to locate anomalies within PDFs' structure and encoding, which indicate that document tampering has occurred. Detect uses several strategies to inform lenders when document tampering has occurred, including:

- Identifying editing software that has been used
- Identifying documents' origins
- Highlighting text that has been added to documents
- Highlighting text that has been overwritten
- Retrieving and displaying the original, underlying document and outlining changes that were made

Q: What should I do when I receive Detect signals?

A: One or multiple signals can be raised to lenders to indicate the presence of document fraud.

- **Note:** the number of signals received does not directly translate to the magnitude or severity of document tampering. One signal may be a strong indication that document tampering has occurred. Multiple signals may help corroborate that document tampering has occurred with malintent. Any and all signals should be reviewed thoroughly.

Clients should review Detect signals raised along with file tampering visualizations when available. We encourage clients to review signals and visualizations via the Ocrolus Dashboard as it provides an interactive and visually compelling experience to aid decision making.

After reviewing Detect signals, lenders should use their discretion to determine what their next steps are, which may include performing any additional review or corroboration of information that was uncovered by Detect.

Q: How accurate is Detect? What is the level of certainty for the signals provided?

A: Detect leverages Ocrolus' sophisticated machine learning capabilities and extensive document dataset (100s of millions of documents) which allows for an unmatched level of accuracy and understanding of file construction compared to other tools and solutions. Detect has been acutely optimized to flag critical anomalies to lenders while striving to minimize false positives[1]. The presence of false positives will vary by lender.

Q: Why do false positives occur and what should I do if I encounter a false positive?

A: False positives can occur for many reasons which may depend on:

- How documents have been handled or saved
- If there are accidental or unintentional edits present
- Whether documents formats are unrecognized or unusual

Lenders should review Detect signals and visualizations within the Ocrolus Dashboard to verify document tampering. File tampering visualizations should allow for quick confirmation or rejection of signals. Lenders should also perform additional verification outside of Detect as they see fit and/or if that is part of their existing workflow or process. If the document tampering cannot be corroborated, lenders should feel comfortable dismissing the Detect signals.

We recognize false positives may be confusing and result in additional time spent on reviews. Please report any instances to support@ocrolus.com which will help us continue to improve Detect and minimize the presence of false positives.

Q: Do you provide a confidence score or assign a level of risk based on the document tampering uncovered? How is this calculated?

A: Yes, Detect returns an Authenticity Score. The score is calculated based on file tampering signals found on the document, their severity in relation to fraudulent outcomes and our confidence in how they were uncovered. Along with the Authenticity Score, users have access to the necessary context as to why a score was returned and can review the associated Detect signals in detail.

Q: Does Detect perform mathematical calculations or reconciliation on the values provided?

A: Yes, Detect identifies balances that do not reconcile and dates that do not fall within the stated period which can be used to identify discrepancies and identify potential fraud.

Q: How do I interpret file tampering visualizations?

A: File tampering visualizations allow for quick and easy confirmation of where tampering has occurred on a document. Detect may provide multiple visualizations per document to help ensure that nothing goes unnoticed. See below for a brief description of visualizations that may be generated.

- **Note:** not all file tampering visualizations will be generated in every instance. For additional details about Detect's visualizations, please refer to our Detect User Guide.

Tamper Overview	Provides an aggregated view of file tampering on the document
Unredacted Document Visualization	Displays when text has been obscured, changes are shown side-by-side
Recovered Document Visualization	Displays received and reconstructed, recovered document side-by-side with tampering highlighted
Added Fonts Visualization	Highlights text that has been added to the document
Tampered Fonts Visualization	Highlights when multiple fonts are identified; multiple colors may be used for each font identified
Overwritten Text Visualization	Highlights new text that has been added over existing text
Misaligned Text Visualization	Highlights when fields are not aligned as expected

Q: How is Detect able to reconstruct and display the original PDF? How often will this be available?

A: The ability to reconstruct the original PDF depends on how it was manipulated. When available, Detect will display the reconstructed, original PDF alongside the received, tampered document to allow for easy investigation of edits that were made.

Q: Why do I see an asterisk next to some documents?

A: An asterisk indicates that the document is non-parsable.