OrbNet Forensic AI

OrboGraph
Intelligent Payment Automation

Forensic Document Examination:
Impact on Banking, Fraud, and Payments

Interview with Khody Detwiler, Forensic Document Examiner

Introduction:

Forensic document examination is foundational for the development of OrboGraph's OrbNet Forensic AI technology. To assist in describing the applicability of forensics in banking, fraud detection, and payments, Joe J. Gregory, Vice President of Marketing at OrboGraph, interviewed forensic expert and author **Khody Detwiler** for a deeper dive into the subject and its impact on banking, fraud, and payments.

Biography:

Khody Detwiler
Forensic Document Examiner
Lesnevich & Detwiler

Mr. Detwiler is an internationally-respected forensic document examiner. His eleven-plus years of extensive experience in both national and international matters are demonstrated via court cases concerning both criminal and civil matters in state, federal, and international courts.

He has been consulted as an expert in all areas of forensic document examination including the identification of handwriting and signatures and the detection of simulated writings and signatures. In addition, he routinely conducts examinations pertaining to alterations, obliterations, and erasures, as well as non-destructive ink, paper, and indentation analysis, among other specialties specific to the forensic document examination field.

Since beginning his career as a forensic document examiner, he has conducted a wide variety of examinations on thousands of individual documents and signatures involved in various litigations throughout the United States and abroad. His international casework has required extensive travel to different locations throughout South America, Europe, and the Middle East. He has been received as an expert and has presented expert evidence on numerous occasions in both state and federal courts throughout the United States and internationally.

Additionally, he also contracts with a variety of state and federal law enforcement agencies, insurance companies, and private entities to perform forensic document examination services on a regular basis.

Mr. Detwiler co-authored chapter 14, entitled "Forensic Analysis of Handwritten Electronic Signatures" in the 2021 publication, Forensic Document Examination in the 21st Century, published by CRC Press.

Click here to review summary and purchase your copy on Amazon.
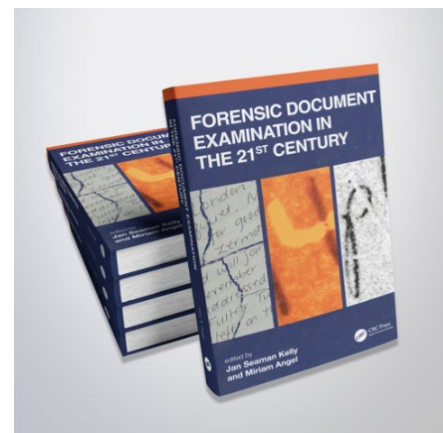
Interview

Joe Gregory:

Khody, thank you again for joining us. Let's start with the fundamental question— what really is forensic document examination?

Khody Detwiler:

Forensics as a whole is the application of science to law. Forensic document examination is a subcategory of the forensic field, dealing with the authenticity of the documents. In a way, it is similar to the ballistics or fingerprint forensic disciplines.

It could involve the examination of signatures, handwriting, a security feature -- as in the situation with passports or travel documents, or identifying the age of a document. What we do as forensic document examiners is analyze documents to make determinations as to authenticity, which could be the document as a whole or some part of the document.

To give you an example of the responsibilities in this field, the scope of my work encompasses: Handwriting/Signature Analysis (Majority of casework), Spectral Ink Analysis – "VSC", Electrostatic Indentation Analysis – "EDD" or "ESDA", Typewriter Examinations, Copy/Fax Examinations, Physical Examinations (i.e., staples pattern and paper), Document Authentication/Verification (security features), Document Reconstruction (Shredded, Charred, and Liquid Soaked), Electronic Signature Analysis (E-signatures), Preparation/Collection of Request Specimen Writings, and Courtroom Testimony.

Joe Gregory:

What an impressive list. What education is needed in order to practice as a forensic document examiner?

Khody Detwiler:

I went through a formal two-year training program that any qualified forensic document examiner will go through. This training is currently published by the Scientific Working Group for Forensic Document Examination (SWGDOC). You can visit their website to access all of the published standards. (https://www.swgdoc.org/)

A large part of the formal training program involves sitting alongside a senior examiner to review every case coming into the lab, complete reading assignments, initiate research, complete a cycle of working cases, and undergo a variety of tests and oral moot courts.

The formal training program covers everything from evidence handling procedures — what you do with evidence when it is submitted to the lab — to how you conduct certain types of specialized examinations such as signature or handwriting analysis, ink and paper examinations, indentation analysis, security feature detection and examination, paper fiber/torn edge matching and comparison, among other specialized examinations.

Joe Gregory:

What is the most interesting type of case that you were involved with?

Khody Detwiler:

The most interesting type of case — personally, I enjoy larger, complex cases that take a lot of time because law enforcement is investigating many moving pieces.

I was involved with was a case out of Saudi Arabia. There were over 100 international banks involved, and what we essentially found is that a group of identical signatures were being used over and over again, on different loan documents across these different banks. Total at stake was a little over $20 billion in that particular case.

What we found was that a mechanical device was being used to replicate the purported signatory's signature on a variety of loan documents. As the case progressed, it became quite fascinating to see how all of the different banking institutions were tied together through this select group of signatures. Our involvement in this matter spanned nearly three years, and I am sure there are parts of this case that are still being litigated today and will be for years to come.

Another of my more interesting cases was a will contest case in which an entire codicil at issue was written entirely in human blood. In most cases, when you think "blood-writing," you think of a crime scene where a victim writes a message in blood to help catch the killer. This case wasn't like this at all. It was actually done with a fountain pen where somebody literally dipped the pen into an ink reservoir full of blood, and hand-wrote an entire codicil.

Joe Gregory:

How can you really identify the differences between handwriting samples?

Khody Detwiler:

If you have two signatures that are pictorially different, before we can get to an opinion that one is not a genuine signature, you have to understand what those differences mean. So, to actually work a case and evaluate differences, we use a sampling of what we call known signatures, or standard signatures. It is similar to how Anywhere Fraud with OrbNet Forensic AI technology works, essentially comparing known standards to the signatures in question.

As a forensic document examiner, I am evaluating whether or not these apparent differences are actually just part of a range of variation exhibited in the genuine signatures of the true author, or if they're actually differences that would be attributed to another writer.

When a difference is noted you have to evaluate — is that difference significant? Or, can it be explained by something going on with the writer at the time of creation, either range variation, maybe there's health issues, an illness — you know, some type of situation going along with that person, that may account for that particular difference.

Now, when you have signatures that are completely different — different in terms of skill, for example, one signature is far less skillful than the other — then you can certainly separate those and say that they're not genuine signatures of the same individual, or one is not a genuine signature due to the fact that writer does not possess the skill necessary to execute the signature in the manner displayed.

The other topic we look at is execution characteristics. For example, if there is an "a" or an "o" that is written as a clockwise formation in one signature, but counterclockwise in the other, that can be a significant difference indicative of two different writers, because the muscular movement of the writing formation is different. Throughout the analysis the examiner really has to take a deep dive to figure out: Is that difference is significant or just part of writing variation?

Joe Gregory:

Can you talk briefly about how 21 discriminating elements ties into this process?

Khody Detwiler:

We have the two different groups that we as forensic document examiners have to look at: pictorial and execution. There are 21 discriminating elements that have been brought out in

literature over the years. For each of those categories, you can have a variety of subcategories.

Part of the discriminating elements are considered to be components of style, or the pictorial features of the writing. For example, features like spacing, sizing, letter formations, are in this category. Here is a listing:

Elements of Style (Pictorial Features)

1) Arrangement
2) Connections
3) Construction
4) Design
5) Dimensions
6) Slant or slope
7) Spacings
8) Class
9) Choice of allograph(s)

The remaining elements are what we call execution characteristics, which is how the signature written or executed. Is it a skillful genuine signature or a slowly drawn simulation? You know, all those different things come into play, when you are looking at that — connective strokes, ending strokes, line quality, and overall writing spontaneity.

Elements of Execution (Writing Habits)

10) Abbreviations
11) Alignment
12) Commencements and terminations
13) Diacritics and punctuation
14) Embellishments
15) Line continuity
16) Line quality or fluency (speed)
17) Pen control (pen position/pressure)
18) Writing movement (including angularity)
19) Legibility (writing quality)
20) Consistency (natural variation and persistency)
21) Lateral Expansion and word proportions

If you're talking about letter formation, for example, that's one discriminating element; however, a signature may contain 15 different letters. So again, now you're looking at all these different letter formations, although it's only tied back to one of the main categories of discriminating elements.

Joe Gregory:

Can you compare and contrast AI software verses how a document examiner works?

Khody Detwiler:

There is a lot of commonality between how software operates and how a document examiner looks at documents and signatures. Tying back to those 21 discriminating elements, the software and examiner analyze similar features such as spacing, sizing, letter formation, etc.

AI software doesn't exactly tell you which features are being analyzed by name. In the case of OrbNet Forensic AI, I know there are 512 feature vectors used in feature extraction which are incorporated with this image analysis. Also remember that software typically analyzes 200 dpi bitonal images in check processing.

aLooking at the check as a whole, the software can certainly run the analysis faster and with greater depth and breadth. When you look at two or three different checks and you are comparing all the spacing elements within the check, i.e. signature lines, margin of the signature line, all these different measurements that software can run automatically. There is no question that it would take a document examiner far longer to complete these examinations with a large sampling than it would the AI software.

The main difference between the software and the human element is that a document examiner can look for specific difficult use cases -- especially with respect to signatures — for example, tracings or a transposition simulation – more commonly referred to as a "cut-and-paste" based on source document attributes and printing processes.

Additionally, we've worked with law enforcement agencies in matters where a booklet of checks get stolen, and we're trying to figure out whether or not certain "cashed" checks tie together, so we can do an impression analysis to see whether or not one check was filled out on top of the other while in the book. This analysis may allow us to also find where other check were being passed which can give investigators additional places together evidence, including possible video footage. We can also examine the ink formulas on a check to determine if alterations occurred as well as security feature verification. Through specialized examinations we may be able to create links between certain items that would not otherwise be possible.

There is certainly a great benefit to the banking industry for software like OrboGraph's to automatically sift or "screen" through volumes of items at a very high rate of speed — things that would take a document examiner days, if not weeks to complete.

In the end, when you combine resources together, that being the OrboGraph software and the qualified examiner, I believe it can be a very foolproof system and an invaluable resource to thwart fraud in any banking institution.

Joe Gregory:

Do you think that the financial industry could use specific programs to help them for fraud review processes or court cases? How about interbank fraud disputes?

Khody Detwiler:

Absolutely. As a comparison, you can think of this process similar to examining travel documents at an airport. First, the TSA agent making the initial contact with the traveler, is confronted with a phony travel document — that's essentially "tier one" or "screening step #1."

They look at it, they'll flag it, that goes back to somebody else who has a little bit more training, a little bit more knowledge, and maybe some more sophisticated equipment than a UV light and a loupe. They then determine that there's definitely a problem, but don't know exactly what it is or how it was done.

The document then gets escalated to "tier three," which would be the forensic document laboratory. And they are the ones who will conduct a thorough forensic analysis of the document to figure out exactly what happened, why it occurred, and what exactly is going on with that document.

Similar to this example, banks should use the software as the initial screening, then use a fraud reviewer — trained by a qualified document examiner, such as myself — to make a pay, hold, or return decision. And for those situations which may involve litigation, a document examiner or crime lab provides a very detailed analysis to substantiate the position of the paying or returning bank.

Joe Gregory:

Khody, I want to thank you again for your time. It certainly was interesting to learn about forensic document examination and the methodology.

Khody Detwiler:

My pleasure, Joe. I look forward to seeing what innovations emerge from OrboGraph in the near future.