See the Unseen:
Inside the Real World of
Document Fraud
Q&A Session

Do you think fully automated document verification can replace forensic experts at the end?

In practice, automation is extremely helpful because it gives speed, consistency, and it can process large volumes of documents much faster than a human examiner.

But from our experience, it does not fully replace expert analysis. Automated systems are designed to detect predefined patterns and known anomalies. An experienced examiner can sometimes notice structural inconsistencies or unusual combinations that fall outside those predefined rules. In the most difficult or borderline cases, the most effective approach is a combination of both. The system performs the initial analysis and highlights potential issues, and then a trained specialist interprets the results and makes the final judgment.

Why is vehicle document fraud often harder to detect than identity document fraud?

Vehicle document fraud is often more difficult to detect because it rarely involves just a single document. In most cases, the identity of a vehicle is defined by several elements at the same time: the physical vehicle itself with the VIN marking, the registration certificate, records in national or regional registries, the ownership history, and sometimes cross-border transactions. Many fraud schemes rely exactly on that gap. The physical identity of the vehicle may already be altered, while the documentation and system records still appear consistent within their own layers. When these layers are not correlated, the fraud can move through the system without immediately raising suspicion.

You mentioned that Regula also provides professional training. Could you briefly explain what kind of training you offer and who it is designed for?

Yes, training is actually a very important part of our work. Our training programs are designed for investigators, border officers, financial institutions, and document examiners who work with identity documents in practice. The goal is to help specialists understand how documents are constructed, how different types of fraud are performed, and what indicators should be prioritized during examination.

The main objective is to develop a structured way of thinking about document verification, so that specialists can identify inconsistencies even in complex or convincing cases. Trainings can be done offline and online as well. More information is available here: https://regulaforensics.com/explore/expert-hub/specialized-trainings/

Question 4

You said different examination techniques today. Do you mainly focus on forensic equipment, or do you also develop software as well?

Answer

Regula works in both areas. Historically, we started with forensic equipment used in document examination laboratories, border control, and investigative units. Over time we also developed software solutions that allow similar analytical principles to be applied in digital environments, for example during remote onboarding or automated document verification.

Today we offer a broad range of document readers and forensic examination devices, as well as IDV software solutions that include document reading and biometric verification.

Very interesting when it comes to printing errors. For non government (online verification) vendors: it's hard to find trustworthy information about these topics. Any insights to combat this?

Printing irregularities can indeed create confusion, because genuine documents sometimes contain small production defects as well.

The key point is that a single printing anomaly does not automatically mean that a document is forged. What examiners usually evaluate is whether the irregularity is consistent with the document's production method and with other elements of the document.

In practice, this means looking at several aspects at the same time: the printing technique used in the document, the behavior of security features, the personalization method, and the overall document structure. Genuine production defects usually appear in ways that are consistent with the manufacturing process, while fraudulent manipulation often creates inconsistencies between layers.

Another critical factor is access to reliable reference material. Having access to a comprehensive database of reference document templates allows examiners and verification systems to compare a document against reference examples and understand what variations are normal and what may indicate manipulation.

How do you protect your verification systems from being reverse-engineered by fraud networks?

We design the system in a way that assumes the client side cannot be fully trusted. Most of the critical verification logic therefore runs on the backend rather than on the client device.

On the client side we also apply several protection mechanisms. For example, the code is obfuscated to make reverse engineering more difficult. This does not completely eliminate the risk, but it significantly increases the effort required to analyze the software.

We also implement different environment checks, such as detecting rooted or compromised devices, which can indicate that someone is trying to analyze or manipulate the application.

Another technical factor is the architecture of the core components. Many of the sensitive parts of the verification logic are implemented in C++, which is significantly harder to reverse engineer compared to higher-level languages.

Overall, the goal is not to rely on a single protection mechanism, but to combine multiple layers of protection that make reverse engineering and large-scale abuse much more difficult.

One of the problems, in several sectors, is that some of the documents that you have to verify do not follow a precise format/layout, they can show the same information in very different ways (e.g. Invoices, Bank Statement), and they have few (or none) security features.

Additionally, in some of these cases it is not possible to verify the information contained in the document accessing external Databases. How would you deal with these situations?

Answer

This is a common challenge when dealing with documents such as invoices, bank statements, or utility bills. Unlike identity documents, these documents usually do not follow a strict format and often contain few or no security features.

In these situations verification focuses mainly on detecting signs of manipulation rather than checking predefined templates. This may include analyzing document structure, identifying inconsistencies in fonts or layout, detecting traces of digital editing, and checking whether the data elements are logically consistent within the document.

Access to reliable reference material is also important. A database of reference examples helps analysts understand typical document structures and identify anomalies.

If a document is examined offline in a forensic environment, additional analytical techniques can be applied. These include spectral analysis of inks, examination under different light sources such as UV and IR, high-magnification inspection of printing characteristics, and even hyperspectral imaging to reveal alterations that are not visible to the naked eye. These types of techniques are commonly used in forensic laboratories and specialized document examination equipment.

Do you think AI will Takeover or replace document Verification Officer at boarding gate?

This is a question that comes up quite often. At this stage, AI is not replacing document verification officers, especially in high-risk environments such as border control or airport boarding gates.

AI technologies are very useful for assisting officers. They can quickly analyze documents, highlight potential anomalies, and automate routine checks. This helps reduce workload and allows officers to focus on cases that require closer inspection.

However, final decisions still require human judgment. Experienced officers can evaluate context, behavioral cues, and inconsistencies that may fall outside predefined automated checks.

For that reason, the most effective model today is not AI replacing humans, but AI supporting human experts. Technology helps identify potential issues, while trained professionals make the final verification decision.

What is the name of the machine that the silver strip was put in to read a VIN number? The machine you said can also read a serial number on a gun?

Answer

The device we demonstrated during the webinar is a magneto-optical VIN examination device, specifically the Regula 7505M.

This device is used in forensic laboratories and by law-enforcement agencies to detect VIN falsification and restore original numbers that may have been scratched, ground, or otherwise altered on metal surfaces.

The technology is based on magneto-optical imaging, which visualizes structural changes in the metal caused by the original stamping of the number. Even if the visible digits are removed, the internal stress pattern in the metal remains and can be detected by the device.

The same principle can also be applied to other serial numbers stamped in metal, including firearms serial numbers, which is why similar equipment is used in firearms examination laboratories as well.

You can learn more about these technologies here:
https://regulaforensics.com/products/vin-and-weapon-examination/

Question 10

As per your experience which is the best technique to verify authenticity of the vehicle.? physical object as you said in presentation. VIN authenticity. and suppose if tampered retrieving the original VIN?

Answer

Verifying the authenticity of a vehicle usually starts with examining the physical VIN on the vehicle itself, including the stamped VIN, VIN plate, and the surrounding metal surface. Investigators look for signs of tampering such as grinding, re-stamping, welding, or other mechanical alterations.

If there are indications that the VIN may have been altered, forensic techniques can be used to attempt recovery of the original number. One of the commonly used methods is magneto-optical imaging, which allows examiners to visualize residual stress patterns in the metal that remain from the original stamping process. Even if the visible VIN has been removed or modified, the internal deformation in the metal can sometimes reveal the original number. This type of analysis is typically performed in forensic laboratories using specialized equipment.

You can learn more about these technologies here: https://regulaforensics.com/products/vin-and-weapon-examination/

Thank you!

Regula

Decades of Forensics for Seamless Identity Verification.
Bringing together 30 years of experience in forensics, border control and business, to create industry standards to trust and follow.