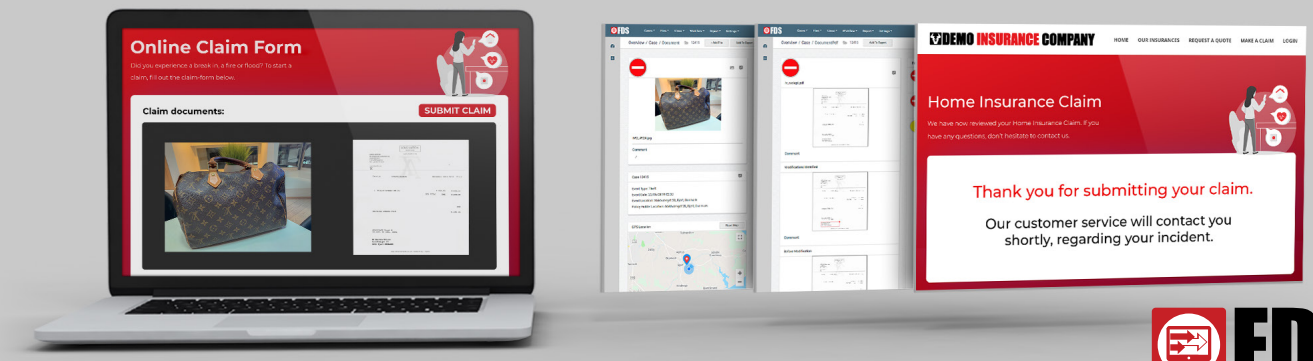


FDS STP
Straight Through Processing

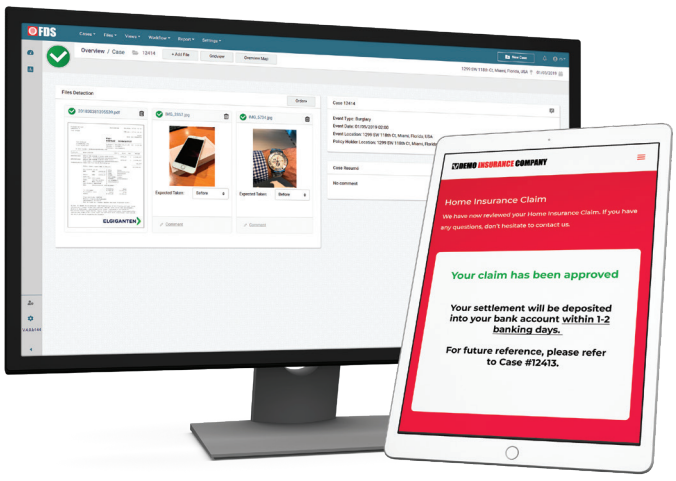
Straight Through Processing the Digital Empowerment

Digitalization must first and foremost make life easier for customers and, at the same time, insurers must rethink how to quickly detect potentially fraudulent claims on file level.

Handle Claims Faster and with Greater Accuracy

Claims handling is a big part of the overall cost in any insurance company. A big part of the expenses associated with claims processes, are caused by inefficiencies in the process of collecting data that is often obtained manually. This results in incomplete or missing data, slow speed of claim handling, and lack of transparency and errors introduced both by the customer and by the data-entry team.

Straight Through Processing (STP) is the next step to claims excellence. Online claims handling and self-service, will make an already stressful situation for policyholders much more hassle-free. This will result in a higher customer satisfaction as the money is paid into the customer's account shortly after the claim has been processed. In the eyes of the customer, claims experience is what insurance is all about.

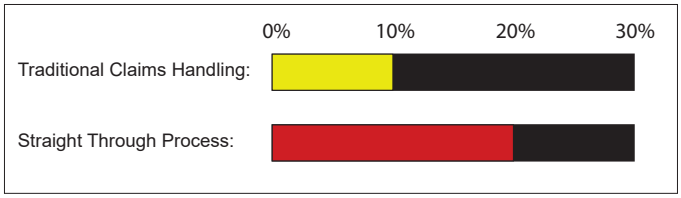


FDS immediately detects if claim documents are genuine or fraudulent

Likewise, STP will reduce the overall claims costs significantly and improve the combined ratio to the ultimate benefit of the policyholder. But not all policyholders are equally truthful.

Fraud and the resources to detect fraud can have a huge impact on an insurance company's combined ratio, as up to 10% of all claims are fraudulent.

Online claims handling is the essential part of any STP strategy - unfortunately analysts expect insurance fraud to double with the rise of automation.



Expected fraud level with the introduction of STP

STP has already given birth to new fraud trends.The way STP expedites the payment process, sheds light on the ways claim automation may heighten the temptation for some consumers to behave fraudulently. Typically, insurers would apply STP logic to claims falling under a certain monetary threshold.

A natural concern regarding low-cost claims would be increased possibilities of fraud on STP claims below e.g. USD 2000, where the pay-out would be less expensive than the costs associated with expert forensic analysis on file level.

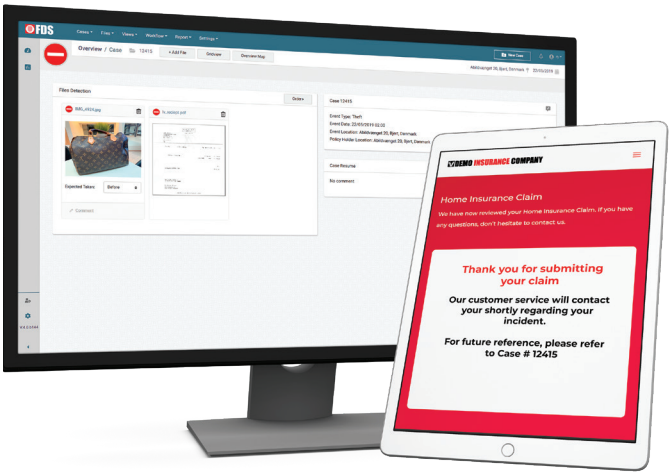
STP - the Ultimate Goal of True Claims Automation

Understanding if claims documents like images and invoices are genuine originals or the result of forgery is not an easy task. Fraud Detect System, FDS, is an evidence-based detection technology based on scientific methodologies to automatically verify the genuineness of claim documents on file level.

FDS should be an integrated part of any STP solution as it instantly determines whether a file is an unaltered original, an original generated by a specific device, or is the result of manipulation through editing software, suspicious geo-location, bearings etc. and therefore may not be accepted as claims evidence.

FDS can detect a multitude of files which include images, invoices, receipts, certificates, health records, employment contracts, warranties and other such documents.

FDS is an extra layer of detection on top of your existing fraud systems, such as business intelligence and AI solutions. Integrated with your STP setup, FDS automatically detects fraud on file level in seconds, using over 100 detection points to verify if documents are genuine or fraudulent. FDS assigns fraudulent claims directly to claims handlers or SIU.



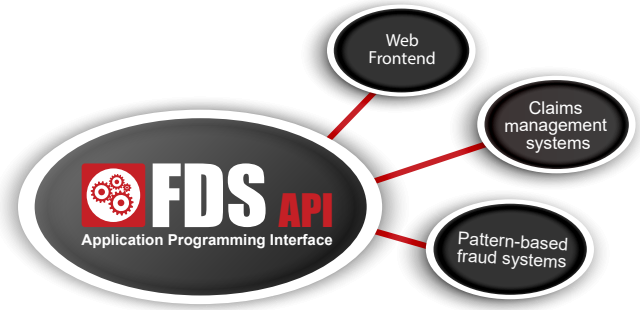
FDS built-in workflow pushes fraudulent claims to claims investigators

Pattern based and behavioral fraud systems are widely used today – however, even though these systems are effective, they also generate false positives. As these solutions usually do not contain evidence-based fraud detection, such claims require costly investigation resources, as they need to be dealt with manually.

By introducing FDS into your STP strategy, you get a very effective extra layer of fraud detection on file level, detecting on e.g. PDF's, images, videos, Word/Excel documents etc.. FDS automates a great deal of the workload and pick-outs that currently require a specialist to manually investigate.

Easy Deployment and Integration

A successful STP project is driven by the ability to integrate systems and work processes i.e. existing claims handling systems, pattern-based fraud detection etc., on top of an intuitive front-end which validates data in a secure way and is "designed by security".



FDS Restful-API makes integration between systems easy

FDS provides a full set of easy adaptable Restful-API (Application Programming Interface) that secure a robust integration. Deployment of FDS is easy and agentless, which means no installation on end points. FDS supports VM environments and can be easily supported by MSP's (Managed Service Providers).

BULLWALL

BullWall is a fast-growing international, privately owned digital innovator with headquarters in Denmark. BullWall is led with empathy and driven by passion, built on talent, dedicated to fight cybercrime in its many forms. Our overarching purpose is to break cyber crime and to combat digital fraud on file level - stop new and unknown strings of ransomware attacks in its tracks - and providing solutions to report data breaches to regulators in a timely manner and secure way.

BullWall's three innovative technologies; RC, FDS and IMS with the sole focus on analyzing and protecting organizations and their digital assets, whether it is protecting against a vicious ransomware attack, detecting advanced insurance fraud or reporting a data breach incident. Our people are the heart and soul of our company. We know what really matters; development, flexibility, recognition, and purpose, always with the customer in focus. BullWall has a global reach and provide cutting-edge technologies to customers within corporate, enterprise, and the public sector.

FDS FDS (Fraud Detect System) is a solution for forensic authentication, detecting fraudulent digital documents and providing evidence based reports on the findings.

IMS IMS (Incident Management System) is a workflow based data breach reporting solution to ensure no human errors or system created data breaches remain unreported or GDPR delayed.

RC RC (RansomCare) is a totally unique Last Line of Defence technology that detects and protects against new and unknown ransomware when other first line of defence solutions fail.

BullWall Ltd • Queen Anne's Gate 34 • London SW1H 9AB • England

BullWall A/S • Oester Snedevej 15 • 7120 • Vejle East • Denmark