INFOPAPER

RISK AREAS TO WATCH DURING THE COVID-19 PANDEMIC

ADAPTING, SAFEGUARDING AND EXPEDITING THE RISK PROCESS FOR COMMUNICATION SERVICE PROVIDERS (CSPs)

The COVID-19 pandemic has brought many challenges to CSPs, including the overload and efficient use of networks, as well as risk management and exposure to fraud. The telecommunications industry softened the effects caused by COVID-19, serving as a reliable means of communication between people and companies. However, the impact of the crisis in other sectors may have adverse economic effects on CSPs in terms of late payments and bad debt. Opportunities for new and adapted forms of fraud have been opened.

It is therefore important to remain vigilant and have proper fraud detection processes and tools in place. Previous exonerating factors such as long-standing customer contracts and non-payment reminders are no longer sufficient indicators during the COVID-19 crisis. These factors were there before, and are now being highlighted and exploited in the framework of this COVID-19 pandemic.

CSPs need to focus on what can be done today to mitigate existing vulnerabilities that have been highlighted during the pandemic and prepare themselves to be better equipped for the uncertain times that lie ahead. A proactive approach is required in order to face the challenges posed by the new "normal".

A first step toward preventing fraud is to create awareness around some of the trends that have resulted from the pandemic and then create an action plan to address the vulnerabilities. Here are some areas CSPs need to pay close attention to as the crisis continues to unfold:

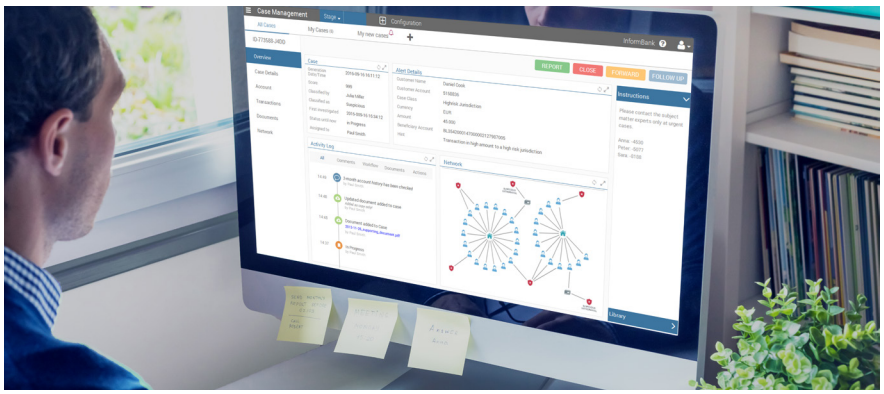
1. **Subscriber Bad Debt:** The economic impacts of COVID-19 have thrust a great number of subscribers into financial hardship, resulting in an inability to pay their bills. Unfortunately, in the current scenario, the situation might extend for years into the future and there is justifiable fear that a bad debt tsunami lurks on the horizon. CSPs need to look beyond and challenge how they are evaluating and managing customers' credit risk, which will require the ability to incorporate new non-financial events in the decision, potentially having to reformulate the models as well.
2. **Payment fraud:** Online shopping at CSPs has been accelerated even further as a result of this pandemic. There has been a new wave of less experienced online shoppers entering the market. There has also been an increase in fraudulent activity – after all, how can CSPs be sure the actual card holder is making the purchase? This is, again, not a new risk but a balancing act that has become a bit more complicated due to an increase in players and changing market dynamics: how can risk for CSPs be minimized without infringing too much on customer convenience?

3. **Application Fraud:** During the COVID-19 pandemic, the social distancing requirements supercharged digital processes and pushed subscribers to rely more, many for the first time, on the internet for everyday processes. At lighting speed, subcribers moved from physical stores to online channels like never seen before. This will likely not be a short lived effect as consumer behavior may have been permanently altered. CSPs had to move to digital-only acquisition and onboarding processes, with greater risks of falling victim to application fraud, including identity fraud and theft. To remain competitive, CSPs need the capabilities to detect application related fraud in real-time with minimal friction.

INFORM is Here to Help

A pandemic can throw even the best risk processes into chaos. It is therefore important to assess current procedures, identify vulnerabilities and keep a finger on the pulse of the fraud trends that have resulted from COVID-19. It is vital to have a fraud detection system in place that can take various data sources into account and triage the attempts that are suspicious, which can then be passed on to the already strained investigative teams. Only those cases that have a high likelihood of being proven fraudulent should be passed on.

This can be accomplished by incorporating proven technologies found in RiskShield such as fuzzy logic, pattern recognition, dynamic profiles and integrating external lists and databases to score fraud attempts quickly and effectively. The more data that can be considered in the decision-making process, the better. Business rules can be enhanced and developed in real-time as new fraud patterns emerge, without any IT coding or system downtime. As behavior changes in the framework of this pandemic, RiskShield can help CSPs adapt, expedite, and safeguard the risk process and prevent fraud.



RiskShield offers a high performance real-time fraud detection engine that is adaptable to new fraud typologies. It is a modular solution that will readily fit with any IT architecture. It can be introduced in one business use case and slowly be rolled out to other application areas.

About INFORM

INFORM GmbH is a global company in advanced optimization software systems and a leader in providing intelligent, customer-centric fraud prevention and AML compliance solutions. With RiskShield we offer a multi-channel platform that detects and manages suspicious activities, minimizing losses and optimizing efficiencies using advanced analytics, machine learning and intuitive rule management controls.

More than 1,000 companies worldwide benefit from using advanced optimization software systems by INFORM in industries such as financial services, insurance, health care, transport logistics, airport resource management and production planning. INFORM employs over 750 staff from more than 40 countries.

For more information, please contact us at:

INFORM GmbH / Risk & Fraud Division
Pascalstr. 35, 52076 Aachen
riskshield@inform-software.com
riskshield.com / inform-software.com
Tel. +49 2408 9456 5000