COVID-19: The Ultimate Vulnerability Check

Using the new light shed on vulnerabilities to create a more holistic fraud and financial crime fighting strategy

Steps Toward Recovery

Our vulnerabilities have been exposed. The threats that are posed to financial institutions as a result of COVID-19 are, however, to a large extent, the same as before the pandemic broke out. Take money laundering in the field of AML Compliance as an example: evading due diligence procedures, misuse of financial aid and emergency funding, using the unregulated financial sector to conceal and launder illicit profits, and so on. This was all happening before the pandemic.

The same holds true for the world of fraud: CEO fraud is on the rise, phishing attacks have increased, applicants for loans and stimulus package benefits are not being honest about company size or even the existence of a company, and the like. These factors were there before, and are now being highlighted and exploited in the framework of the COVID-19 pandemic.
Financial institutions 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. Awareness creation is the first step toward mitigating vulnerabilities, action is the next and most important step. Here are a few places to start:

**Money Laundering and Increased Money Mule Activity**

Whether through a digital fraud scheme such as work-from-home-scams or using a direct approach, money launderers are taking advantage of people in desperation during this pandemic. Their recruits are often initially unaware that they have become the so-called money mules. The true victims are often not visible to those that may even willingly become money mules, so justifying a few deposits and money transfers becomes easier as the illegal activity behind the dirty money seems so far away.

Pandemic or no pandemic, this activity is illegal, and it needs to be stopped by financial institutions. Banks, insurance companies and payment processors, even before the pandemic, struggled to have successful anti-money laundering procedures in place. The cracks and vulnerabilities in current strategies are just now being highlighted and exploited at a higher rate due to COVID-19. A main contributing factor is a lack of collaboration across departments and missing communication amongst the various tools being used within the compliance process. Managers must implement a holistic compliance process to best manage risk across all business lines and customer accounts, and deliver an enterprise-wide view on their customers and portfolios.

This can be accomplished through increased transaction and behavior monitoring. It goes back to the key to any sound anti-money laundering strategy: **Know Your Customer**. If nothing else, this crisis should be a stimulus for many organizations to begin improving their AML Compliance strategy.

---

The Benefits of Having RiskShield for AML Compliance

- A complete package solution that can be easily adapted to specific requirements
- Taking a holistic approach to monitor all customer activities on a single platform
- False positive reduction using smart AI algorithms
- Data sharing between modules to make more accurate and informed decisions
- Possibility to enhance decisions with machine learning

---

**NOW IS THE TIME FOR THE ULTIMATE VULNERABILITY CHECK-UP**

---

*Ongoing Customer Due Diligence*
**Lending and Solvency Checks**

With or without a pandemic, having a sound solvency check workflow in place should be a priority for banks and other financial institutions. As few barriers to loans as possible were necessary to save many small businesses in the initial phase of this pandemic. This unfortunately resulted in many fraudsters across the globe making profits from the capital injections into the international markets through the filing of fraudulent applications. Now is the time for financial institutions to look at how the risk associated with further stimulus and loan application activity can be minimized. This begins with an appropriate solvency and identity check process. It is important that the process is not an additional barrier to legitimate companies that require funds, but rather a facilitator for quick approval or denial. Detailed checks to understand if the applicant has previously applied with the financial institution must be made. Applicant detail comparisons should be executed to determine if there is a match on any third party or internal fraud blacklists. Pattern analyses can be used to determine if the behavior of applicants matches a previously known fraudulent application.

As many data sources as possible need to be integrated into the process, and the key to all of this is that it must be executed in real time! The result will be fewer loan defaults, happy legitimate businesses that receive funds quickly and frustrated fraudsters that are suddenly being denied.

---

**E-commerce Fraud**

E-commerce shopping 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 merchants 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 merchants and payment processors be minimized without infringing too much on customer convenience?

Risk-based authentication can help. The goal is to process as many payments as possible without additional authentication, ensuring a positive shopping experience, but requesting a “step-up” verification for uncertain and risky transactions. The introduction of additional data points through 3D Secure 2.0 allows for a holistic view of the customer and online transaction for a more accurate risk analysis.

---

**The Benefits of Having RiskShield for E-commerce Fraud Prevention**

- High performance and real-time fraud detection
- Fast adaptability to new fraud typologies
- Advanced decision engine with efficient in-memory technology
- Modular solution that will readily fit with any IT architecture
- Full control of rules management without IT involvement
COVID-19 RESPONSE

Hybrid AI for Financial Crime Prevention and Detection

There are several mentions of “available data” and “data sources” in the previous sections. Machine learning models require ample data to be able to learn. With numerous behavior changes by merchants, buyers, and criminals resulting from the pandemic, the required data for detecting fraud and other criminal activity may not always be readily available. However, with industry experience gained over many years, best practice knowledge-based rules can be implemented to detect and prevent fraud and other illegal activity within the payment and online transaction ecosystems. As data pools grow, machine learning can step in to enhance risk and fraud detection capabilities and help identify new modus operandi. The Hybrid Artificial Intelligence Approach takes the best of the knowledge based and machine learning worlds to create a powerful financial crime fighting strategy.

The COVID-19 Vulnerability Check-List

Our financial crime fighting experts are here to help. Please do not hesitate to reach out with any new or old vulnerabilities you have discovered as a result of the COVID-19 pandemic. We are happy to consult and support where we can. If you are at the beginning of your assessment of risks, here are a few places you can begin looking:

- Criminals are taking advantage of a crisis, it’s even more critical to remain vigilant for any exploitation of your systems and infrastructure.
- Review your risk indicators and thresholds regularly and adapt accordingly, especially during changing conditions and circumstances.
- Stay alert of any changing behavior of your customers during the crisis.
- Implement a flexible risk-based approach to mitigate your risk associated with financial crime.

Use Case Highlight:

German State & Development Banks have been hit by fraudsters who have now taken advantage of the coronavirus emergency funds that were supposed to be helping freelancers and small businesses. This is, not a localized problem. Banks across the globe, both private and public, are facing an unprecedented challenge with the influx of emergency loan applications.

RiskShield can help quickly address this problem with its real-time fraud detection and data reconciliation capabilities. The number of credit applications based on IP address, device ID and recipient accounts, along with numerous other factors, can be rapidly assessed using decision modeling supported by fuzzy logic, scorecards and the like.

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.

Contact Us

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