



ShuftiPro
Identity Verification

How businesses can prevent fraud during **COVID-19**



“

*Amid the **COVID-19** outbreak, we can't sit quietly and see businesses shutting down right and left. **Our AI-powered KYC verification** solutions are the right fit for businesses looking forward to onboard secure clientèle. Our contact-less products aim to ensure that when everyone is panicking, fraudsters and terrorists don't take advantage of the situation.*

Victor Fredung, CEO Shufti Pro

”

Contents

Cyber scams are on the rise amid COVID-19 pandemic	02
Financial Authorities have been issuing warnings	06
Increasing risks of fraud	09
Low cyber resilience	12
Data and security risks	13
AML and CDD	15
What strategy should be adopted?	16
Shufti Pro is assisting firms to fight back against fraudsters	18
References	19

Cyber scams are on the rise amid COVID-19 pandemic

The coronavirus pandemic is an event causing stress and imposing unannounced changes for the businesses all across the globe. Be it financial, operational, supply chain, automotive or any other commercial industry, each of them is affected by the virus both in operational capacity and financial stability. Against this backdrop, the financial services sector is having to adapt at scale and rapidly to current constraints and market conditions.

As of now, the organisations have understandably emphasised instant financial and operational measures like controlling cash flows, protecting liquidity and ensuring that they are able to keep core business activities going on.

As the situation evolves, we expect to see a shift in focus and a re-prioritisation of operational and conduct risks as firms come to terms with managing dispersed workforces.

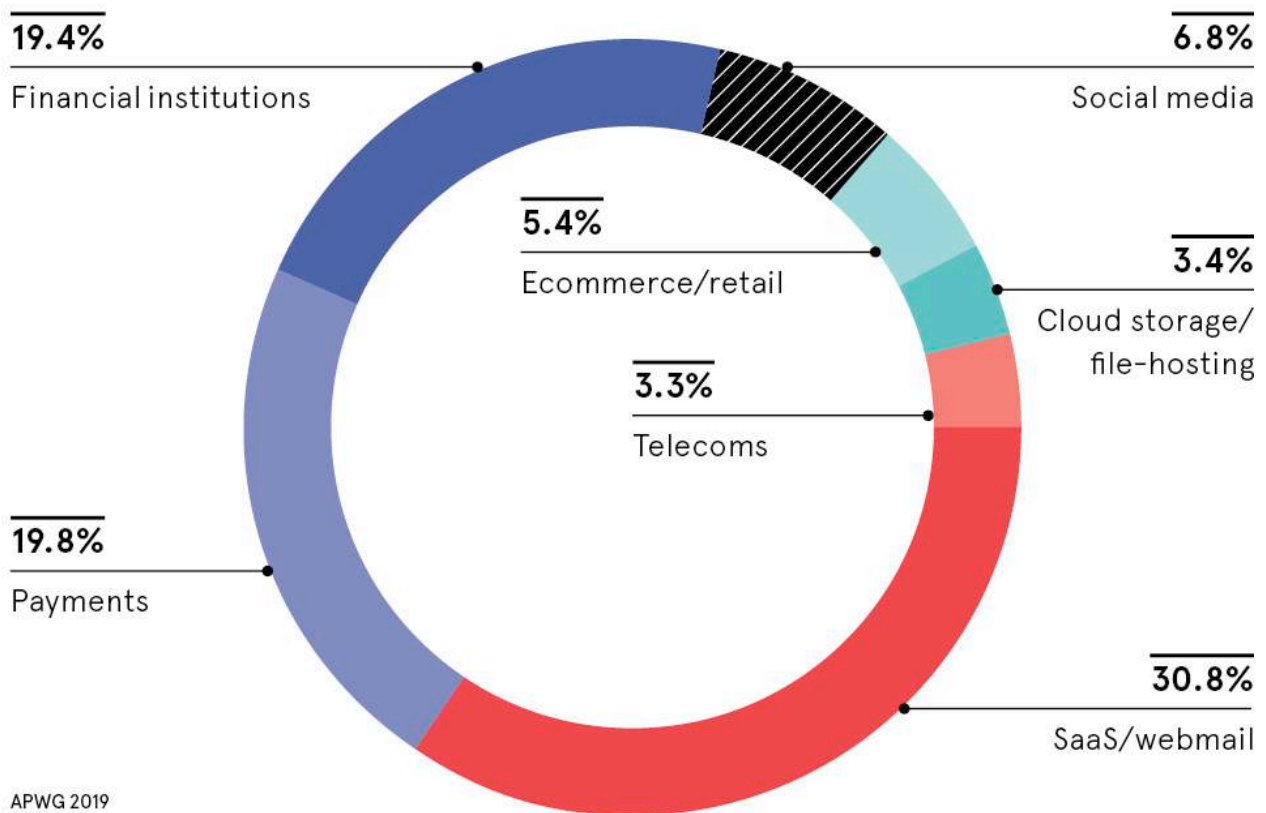
In this paper, we will discuss the increasing risks to the businesses and especially how different sectors are responding to emerging threats such as fraud, data breaches, phishing attacks, fake identities and account takeover frauds.

Acknowledging these strains faced by the businesses, financial regulators have taken positive steps to alleviate the pressure, postponing some high impact checks and activities including stress tests, reducing capital buffers, and delaying non-critical supervisory reviews where possible.

The increasing number of cybersecurity attacks are making authorities worried about the situation, which is why the officials are issuing warnings on their platforms. [Action Fraud reported](#) that since Feb. 1, it's received **105 reports of crime** with a coronavirus or COVID-19 theme, with reported losses reaching nearly **£970,000 (\$1.14 millions)** [1].

MOST TARGETED SECTORS BY PHISHING ATTACKS

Share of total phishing attacks directed to the following sectors/industries



"The majority of reports are related to online shopping scams where people have ordered protective face masks, hand sanitizer and other products, which have never arrived," the report says.

The cybercrimes aren't only increasing in European countries, the USA is also badly affected by the increasing number of cyber frauds during COVID-19. The FBI's IC3 or Internet Complaint Center issued a warning on April, 13th indicating that BEC scams might increase during the pandemic [2]. Previously in 2018, global losses due to Business Email Compromise (BEC) fraud exceeded \$12.5 billion.

The disruption caused by COVID-19 outbreak in market and demand precise attention to the potential financial crimes, scams and other fraudulent activities such as potential misconducts (i) by insider traders triggered by increased opportunities created due to the crisis; (ii) by fraudsters and cybercriminals (e.g., social engineering and phishing preying upon current uncertainty and fear among the people.); or (iii) by financial crimes resulting from the reductions and relief in compliance monitoring and controls due to the crisis).


Warnings from Financial Regulatory Authorities



The regulators are issuing warnings worldwide that the COVID-19 outbreak may result in a large scale increase in financial crime and other misconduct as the disturbed market conditions, reduced staff and other such factors disrupt the economic growth, similarly like it was observed during the past economic crises.

United States Department of Justice (DOJ) on March 22, 2020, announced the first enforcement action against COVID-19 related fraud after receiving directions from the Attorney General to **“prioritise the detection, investigation and prosecution of illegal conduct related to COVID-19 pandemic.”** [3]

The Financial Crimes Enforcement Network (**“FinCEN”**), Financial Industry Regulatory Authority (**“FINRA”**), U.S. Securities and Exchange Commission (**“SEC”**), and Commodity Futures Trading Commission (**“CFTC”**) have all advised financial institutions to be on high alert for a potential increase in **“illicit financial activity”** and have issued guidance that financial institutions can utilize to reduce instances of financial crime and misconduct. [4]



guidance that financial institutions can utilize to reduce instances of financial crime and misconduct. The authorities jointly issued a statement warning the organisations to **verify the investments** especially in crypto-related trading.

FINRA has gone a step ahead by providing the member organisations regulatory relief and pandemic related guidance, asking the member firms to maintain appropriate supervisory and cybersecurity practices [5]. FINRA also pointed member firms to prior guidance on pandemic preparedness [6].

FinCEN has warned the institutions to remain alert about malicious and fraudulent transactions [7]. The authority also reported that a lot of scams (impostor, investor, and product) are emerging during the **COVID-19** pandemic and advised the financial firms to reference its prior guidance and reports on financial crimes during natural disasters [8].

SEC and CFTC issued warnings to the potential investors about the investment scams related to coronavirus. The document provided helpful tips on identifying the fraudulent investment opportunities [9].

In Europe, the European Banking Authority (**EBA**) has emphasised on the fraud and other risks related to payment services during the crisis, when purchasing on the internet is increasing and reminded consumers of the EBA's and national regulators' key tips regarding the choice of financial products and services, which could also be relevant and applicable to other purchases in order to protect consumers [10].

The French authorities **ACPR** and **AMF** issued warnings to the public about the scams that could emerge during the COVID-19 outbreak and the downturn in financial markets. Regulators also notified investors to take precautionary steps and vigilant measures before investing [11].

The European Securities and Markets Authority (**ESMA**) and the **AMF** also recommended the businesses to follow and comply with the guidelines issued on compliance obligations having a direct impact on financial misconduct during the COVID-19 crisis [12].

The **AMF** imitated ESMA's recording guidance and issued its own advice to the regulated financial entities to remain vigilant of **remote working situations** during the crisis [13]. The AMF also invited market participants to contact it with potential difficulties with complying with regulatory obligations during this period, including difficulties relating to compliance obligations designed to prevent, detect and report potential financial misconduct.



Increasing risks of fraud

The financial services industry is at a high risk from heightened levels of fraudulent activities, including cyber frauds, as criminals attempt to exploit the COVID-19 pandemic.

Following the recent announcements regarding the emergency measures, the number of applications from both individuals and businesses to accept support schemes are going to be increased significantly. One of the major concerns is that these claims may be made fraudulently, but processed rapidly, with less stringent regulatory obligations (see **AML** and **CDD** section below).



If approved, funds may be transferred rapidly and with the whole system under stress, recovering funds due to fraud may be a relatively low priority.

The National Crime Agency (**NCA**) in the UK has issued an **update** related to the COVID-19 scams [14]. The report, in particular, mentioned that it is expected to see an increase in Authorised Push Payment (**APP**) frauds, sometimes also referred to as bank transfer frauds. In 2019, a total of £456 million was lost to APP fraud, split between personal (£317 million) and business (£139 million) accounts.

UK Finance has called for **cross-sector cooperation** to fight the rise in APP fraud, and banks and payment providers will need to be alert to the reputational risks of their brands being compromised by association with this type of activity [15].

The Federal Conduct Authority (**FCA**) issued advice for the consumers on scams related to COVID-19, noting that scams may take many forms including the ones that are previously unknown.

In particular FCA mentioned that the scams could relate to insurance policies, pension transfers, investment schemes with high returns, **money laundering tactics** that may include investments in crypto assets.-The authority also mentioned that the scammers are sophisticated, persistent and are likely to target the most vulnerable.

The risk of internal fraud will potentially increase due to remote working and associated reduced oversight and challenge.

Low cyber resilience

Cyber attacks swelled, ranging from the phishing attempts to social engineering tactics and resulting in **identity theft, account takeover frauds** and other financial frauds. Cybersecurity experts are mobilising globally to provide threat intelligence and combat these attacks.

Shufti Pro is offering online **fraud prevention** tools based on AI technology to help firms deal with these kinds of frauds.



More than ever, firms will need to shore up their cyber defences and educate employees, at all levels, to the emerging risks and adopt new digital technologies.

Data and security risks

As remote working becomes the new norm, businesses need to look around for new ways in which data is accessed. Alongside the cybersecurity issues mentioned above, employees are now potentially working with the sensitive data in less secure home-based environments. The balance between locking data down securely behind a corporate firewall and making it more open and readily accessible, to employees and business partners, need to support new ways of working to keep existing business processes and operations moving.



Work From Home the New Norm

In the past, many firms have been attacked and compromised due to low security and with remote working becoming necessary, it's high time businesses invest in acquiring and implementing new technologies capable of preventing **data breaches**.

Regulations such as **GDPR** still apply, so Risk and Compliance heads will need to re-evaluate the associated risks accordingly and potentially deploy alternative mitigation measures.

AML and CDD

There may be new challenges for firms in running AML and CDD activities remotely or on-site but with drastically downsized teams due to social distancing measures.

Common checks may not work as they should for a number of reasons:

- Controls may be weakened by disjointed processes and remote working.
- Where manual checks are required, there may be delays due to technological constraints or unavailability of authorities.
- With unavailability of the advanced technologies performing AML and CDD might not be possible.

Even though that current scenario presents a lot of challenges for CDD and AML screening, the UK regulators have not made any concessions to AML or CDD requirements, therefore firms will need to ensure that they still maintain robust processes around these activities.

What strategy should be adopted?

An unexpected outcome of the COVID-19 situation may be a temporary relaxation of the regulators' focus on promoting competition. This may also apply outside financial services as the government and regulators encourage firms and industry bodies to collaborate in order to facilitate effective crisis-management.

It is uncertain how long the current situation will last, but we may be in this for the long haul and the impacts may be enduring, so firms will require long-term adjustments to working practices and culture.

Whilst there will undoubtedly be further regulatory guidance in many areas, firms will need to be proactive in assessing and addressing the new emerging risks and the changing priorities.

Businesses need to shift their focus towards digital transformation. Adopting contactless payment solutions and contactless forms of customer verification and authentication will be helpful in their digital journey.

Moreover, with the great emphasis on the contactless means of transactions and prevention of frauds including identity theft and account takeover frauds, online identity verification and customer due diligence online is what businesses should adopt. Online verification of the customer to prove who they say they are without any physical and face to face interaction will help solve the online identification issues.

Shufti Pro is assisting firms to fight back against fraudsters

Shufti Pro with its suite of technologies to protect financial institutions and digital businesses has been helping organisations to fight fraud including credit **card frauds, identity scams, money laundering and terror financing.**

The institutions need to incorporate KYC alternatives for the successful onboarding of real customers and fraud mitigation. These alternatives include Shufti Pro's **video KYC, Digital KYC verification and AML screening solutions.**

[Contact Now](#)

[Get Free Trial](#)

Have questions? Contact us and learn how we can help you.



www.shuftipro.com



sales@shuftipro.com

References

- 1 <https://www.bankinfosecurity.com/coronavirus-cybercrime-victims-please-come-forward-a-13992>
- 2 <https://www.ic3.gov/media/2020/200320.aspx>
- 3 <https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud>.
- 4 <https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions>
- 5 <https://www.finra.org/rules-guidance/notices/20-08>
- 6 https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus
- 7 <https://www.cftc.gov/coronavirus>
- 8 <https://www.finra.org/sites/default/files/NoticeDocument/p120207.pdf>
- 9 <https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf>
- 10 https://eba.europa.eu/sites/default/documents/files/document_library/0.%20EBA_Factsheet%20for%20consumers_Final_New_0.pdf
- 11 https://acpr.banque-france.fr/sites/default/files/medias/documents/20200326_communique_presse_acpr_amf_vigilance_arnaques_coronavirus.pdf
- 12 <https://www.amf-france.org/en/news-publications/news/market-activities-continuity-during-coronavirus-pandemic-amf-states-its-expectations>

- 13 <https://www.esma.europa.eu/press-news/esma-news/esma-clarifies-position-call-taping-under-mifid-ii>
- 14 <https://nationalcrimeagency.gov.uk/news/fraud-scams-covid19>
- 15 <https://www.ukfinance.org.uk/uk-finance-cross-sector-cooperation-needed-tackle-rise-authorized-push-payment-fraud>



Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from [3000+ ID](#) templates and business entities from [200 million](#) companies data.

Disclaimer: No warranty or claim is herein provided that information contained in this document is accurate, up-to-date, and/or complete. All information provided in this document is limited for general informational purposes only. In no circumstance(s), does such information constitute as legal or any other advice. Any individual or company who intends to use, rely, pass-on, or re-publish the information contained herein in any way is solely responsible for the same and any likely outcomes. Any individual or company may verify the information and/or obtain expert advice independently if required.