BIK
BIURO INFORMACJI KREDYTOWEJ

experian

Fraud prevention responses for the COVID-19 crisis

Introduction

"Currently businesses throughout EMEA face challenges from reduced business volumes and unseen degrees of digitization. Even if the current Fraud levels seem lower than in the past, they are expected to grow substantially in the near future.

Today, many businesses are working to improve their Fraud prevention capabilities to be prepared for increasing Fraud volumes and new Fraud patterns. Now is the time to start designing strategies that will prevent damage to organisations and individuals."

Marek Miller – Managing Director CEE, Experian

"The awareness of cyber threats is increasing, but it was the COVID-19 pandemic that pushed the business world to intensify efforts to strengthen protection against cyber-attacks. This applies primarily to the financial market, natural BIK playground. As one of key infrastructure entities, we support banks, other financial institutions and their clients in the area of protection. Anti-Fraud Platform and BIK Alerts are our flagship solutions successfully fulfilling clients expectations.

Cooperation is the key to success in this fight, only thanks to it we can strengthen the protection of the entire sector and minimize losses."

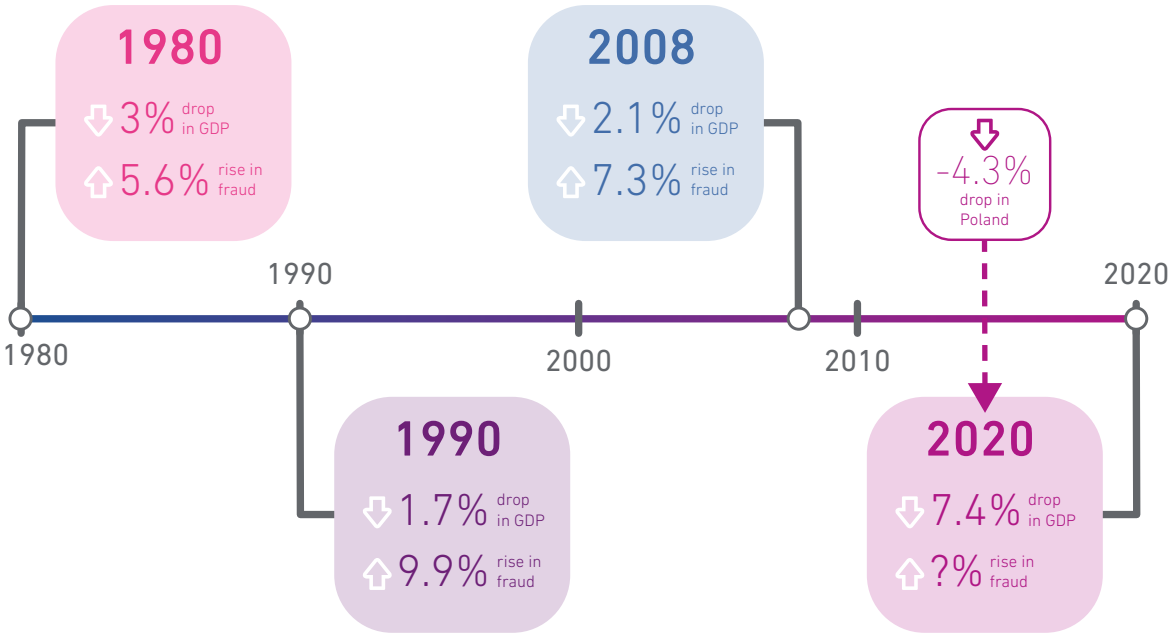
Mr. Mariusz Cholewa, PhD, President of Biuro Informacji Kredytowej and President of the Management Board of ACCIS (Association of Consumer Credit Information Suppliers)

Fraud prevention responses for the COVID-19 crisis

The current global health crisis has impacted societies and business in an unprecedented way. In contradiction to previous economic downturns, the current situation is not triggered by financial indicators but by the health situation. Still, the impacts are like the ones experienced in the previous, purely financial, crisis and the Fraud exposures also follow trends that were either known for a long time or had already started during the last year. A UK University study analysed previous recessions and accompanying fraud correlation.

Organisations must also be prepared for a variety of fraud types associated with legitimate consumers. This can include applying for credit without an ability (or even the intention) to repay, manipulating application information to qualify for credit, making fraudulent claims against legitimate policies (COVID-19 cancellations of travel, weddings, hire, rental etc.) and even in some cases individuals in financial distress and agreeing to co-operate with organised crime (act as money mules).

The increased pressure being put on organisations at this time via higher volumes of customer service requests will inevitably mean that some companies will be less attentive to fraud attacks as they focus on "keeping the lights on" with customer service and other activities.



Source: Centre for counter fraud studies, University of Portsmouth

Fraud levels in March 2020

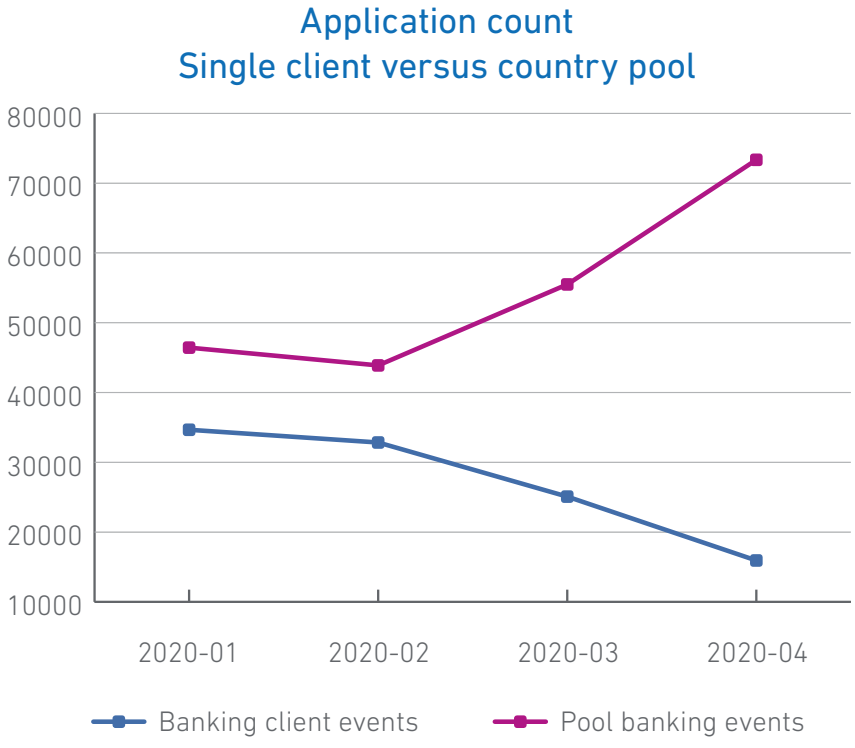
At the peak of the first COVID-19 wave in 2020, business lock downs and social distancing is dominating global economy. The feedback of several market players is similar – business volumes are down, nearly no Fraud attacks are experienced. That results in businesses concentrating on liquidity topics fully. At the same time, resulting from that basic need, new and previously ongoing initiatives to transform existing business to digital are initiated and accelerated.

The lower volumes in financial Fraud, currently experienced, shifts attention within risk prevention to credit and operational risk types – this holds substantial risk. During the last economic liquidity crisis in 2008 similar trends and situational analysis led to substantial losses in later phases.

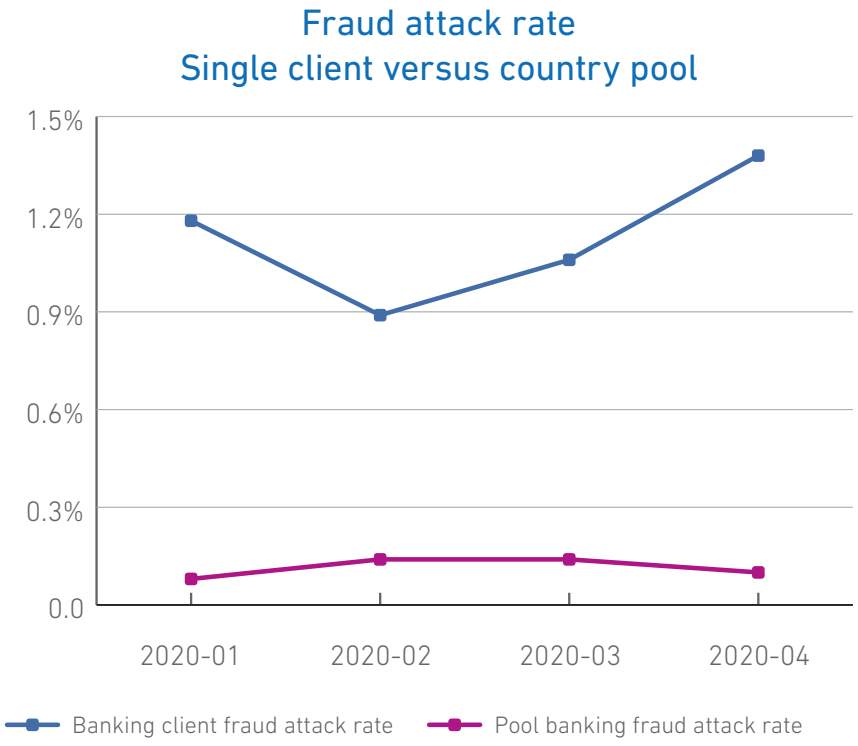
As a result in March nearly all criminal activities were delayed.

For many businesses Fraud exposure has changed dramatically in the second half of April. While new business volumes are still recovering at many organisations, Fraud levels reach new highs in comparison with 2019.

In April the picture is still mixed – market trends and single clients' fraud exposure do not always meet:

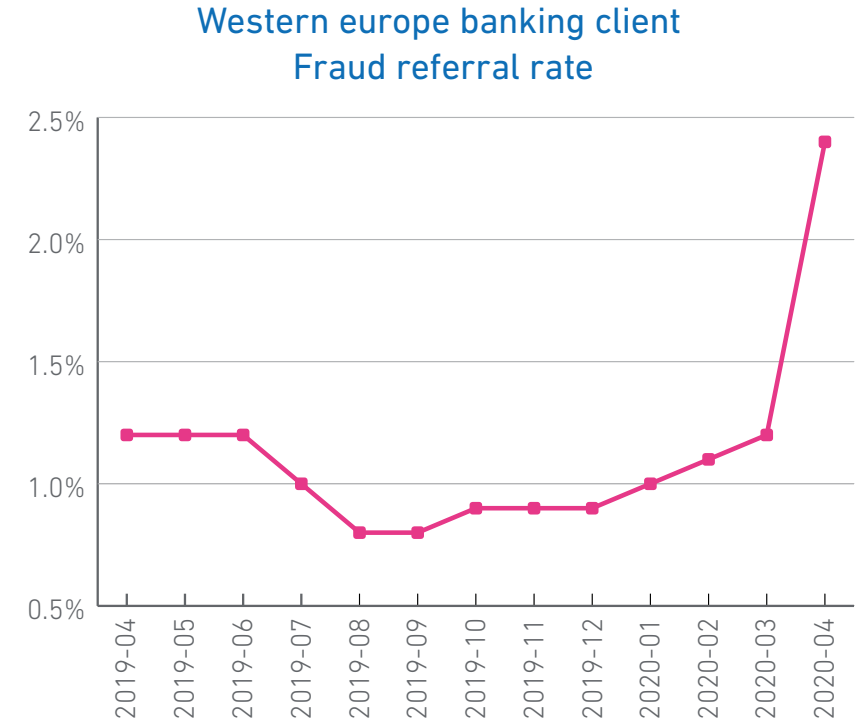


Source: Experian fraud prevention pool solution Eastern Europe

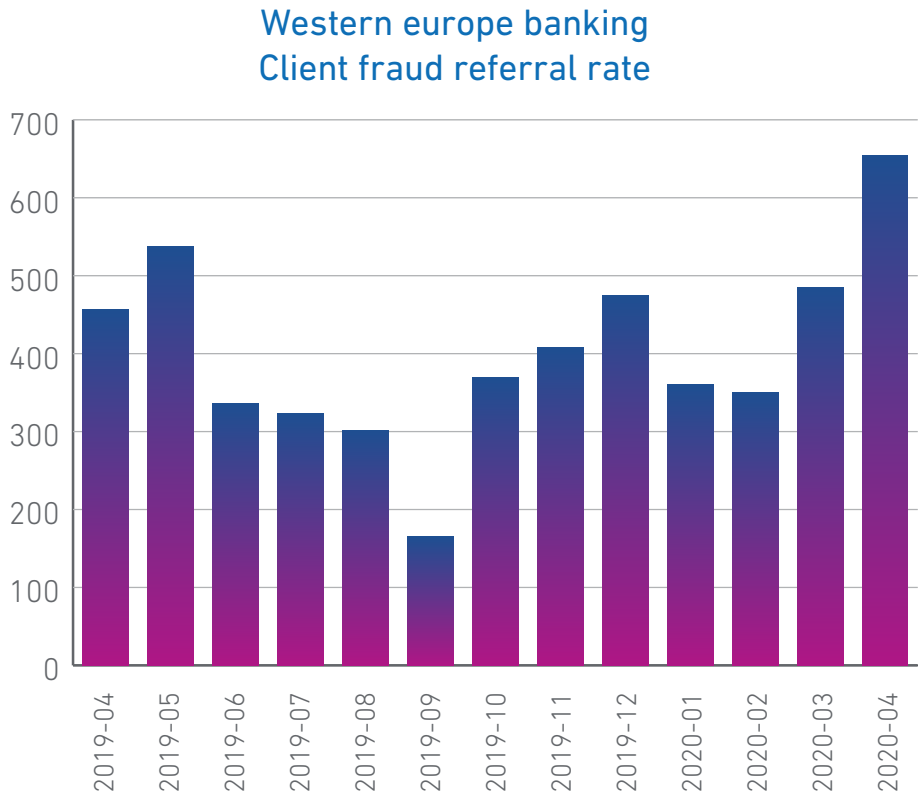


Source: Experian fraud prevention pool solution Eastern Europe

In general, a high amount of suspect applications still meets prevention processes with substantially reduced capabilities due to current restrictions.



Source: Experian fraud prevention pool solution Eastern Europe



Source: Experian fraud prevention pool solution Eastern Europe

Digital channels' fraud

Obviously, criminal activities focus on goods, products and channels with the lowest risk. Even though, non-digital channels within financial and other industries are operational, they are limited and less frequently used.

This, in general, raises the risk for criminals that their activity will be detected – this is one of the drivers that lead to lower levels.

Also, before the COVID-19 outbreaks, digital channels raise in attention of criminals around the globe, as they usually provide the main characteristics easing criminal activity (digital and non-digital).

The key words are not new, not even for the digital age, but are increasingly important in times of isolation

- **Fast** (optimised and partially automated decision processes)
- **Street** (so products that are available for new to business customer from the "street")
- **Cash** (products that are paid out or can be re-sold easily, like telephone SIM cards)

The current risk for consumer data

Criminals acting anonymously online are exposing weakness caused by current fear. Scams, phishing and malware are just some of the tactics being used by hackers. Immediate financial gain and access to data are the targets of their efforts. Whilst the broad techniques being used are not new, the rate of attack has increased notably and, with it, the risk to consumers' data and the threat to businesses dealing with those consumers in a digital marketplace. In a recent article Europol identified the following factors that play a role in the increased threat of fraud:

- **High demand for certain goods**, PPE (personal protective equipment) and pharmaceutical products
- **Decreased mobility** and flow of people across and into the EU
- Citizens remain at home and are increasingly **teleworking**, relying on digital solutions
- Limitations to public life will make some **criminal activities less visible** and displace them to home or online settings
- Increased anxiety and fear that may create **vulnerability to exploitation**

Organised crime groups adapted very fast and created a threat scenario for the current times. These include:

COVID-19 Health Scams

Scammers using fear to access data and money

- World Health Organisation (WHO) emails offering protection advice and asking for donations towards WHO research
- Links offering details of local COVID-19 victims, but leading to malicious code, website and ransomware

COVID-19 Coping Mechanisms

Scammers using offers to gain data and money

- Offers of government benefits, grants and coping mechanisms
- Claims management – companies offering to manage holiday and other insurance claims
- Offers to move money to less risky investments
- Offering additional life insurance but providing no service
- Guaranteed credit applications for an advance fee (and no service provided)

COVID-19 Lifestyle Offers

Scammers offering digital services for homelife

- Offers for subscription and media services (such as Netflix, I-tunes, Xbox live etc.)
- Account update requests (password, credentials)
- Refunds on unused subscription services (e.g. TV Sports Channels)
- E-commerce offers (often 'too good to be true')

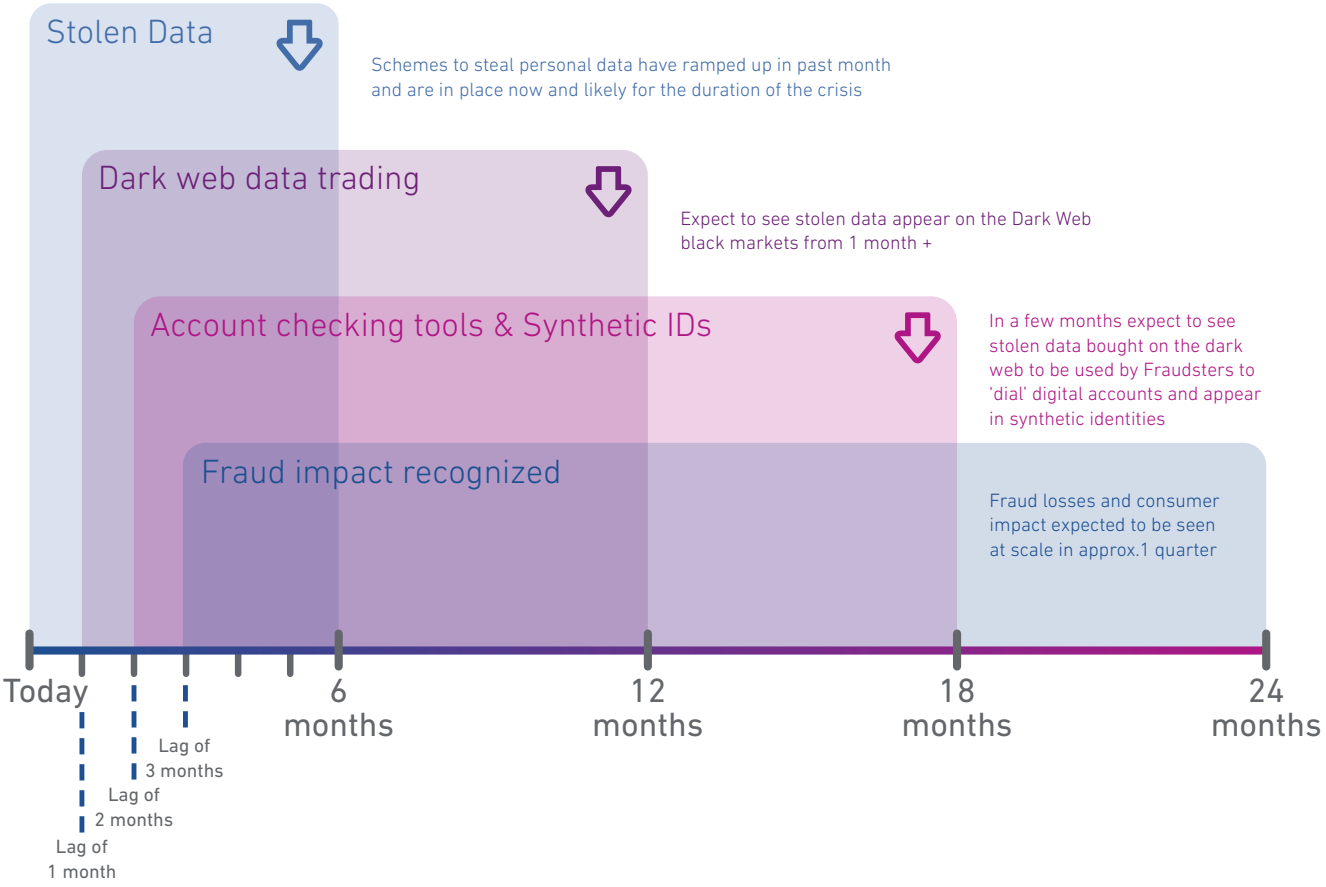
Source: Experian Fraud & Identity consulting EMEA

Fraud prevention responses for the COVID-19 crisis

Criminals have reacted very rapidly to the opportunities presented by the COVID-19 crisis to launch a series of cyber-attacks against organisations and individuals, including phishing campaigns that distribute malware via malicious links and attachments, and execute malware and ransomware attacks that aim to profit from the global health concern.

Access to personal data in this way allows the criminal to exploit an identity, taking over accounts, creating new applications or even creating synthetic identities using some legitimate data. This creates the opportunity for longer term, more extensive gain.

The 'Fraud life-cycle' is an on-going process, the specific impact of COVID-19 could be felt for as long as 24 months from now. The immediate emergence of new fraud schemes and a further increase in the number of victims targeted can be expected. Even when the current crisis ends, criminals are likely to adapt fraud schemes in order to exploit the post-pandemic situation.



Source: Experian Fraud & Identity consulting EMEA

Polish fraud exposure is part of global trends

BIK has conducted an holistic survey* on the expectations of Polish citizens on the impact of the COVID-19 pandemic.

It shows growing concerns of the further development of the financial crisis. Already in this early stage 66% answered that they see a negative impact of the financial crisis to their home budget and 44% foresee problems paying their bills. These fears peak in the age range of 45-54, a group of individuals not counted as main risk group for corona virus, but in the centre of society.

It is notable that an increased digitization in everyday use of business transactions is reported by the survey– already 29% of polled individuals have increased their number of online transactions by now. This number is expected to increase during the crisis.

Cyber-fraud is currently on the rise globally. The BIK study found a significant proportion of Polish citizens had experienced phishing emails. 30% received suspicious emails asking them to click a link or download a file or know a person who has encountered similar fraud attempts. 9% encountered or know about an attempt to steal personal data but a comparably low 7% of polled individuals had experienced a situation of a fraudulent subscription.

Consequently already 29% have raised their attention of bank account access – email accounts, IT devices and social network accounts follow with 24 and 23%. A very high 66% of individuals stated that they pay higher attention on the correctness of web addresses to prevent Fraud. Its important to understand that these messages are mainly supported by the age group 55-64 which are the main targets of certain up to date Fraud schemes. This age group also shows the highest awareness for the fact that they are on current fraud trends – the highest approval rate is found in the age group 65+.

On the other hand, 25-34% have not changed their security measures in the same degree but are expected to have had higher awareness already in the past.

Only 14% do not apply antivirus software and do not plan to install such in future.

It is important to understand that even individuals that have a low digital profile are potential victims of cybercrime – to a certain degree even more. As soon as an individual's data is available on digital platforms, it is at risk of compromise. Less technically educated people also have fewer means to detect ongoing crimes and are therefore easy victims to a certain degree.

*The study carried out on behalf of BIK, on March 18-19, 2020, Research & Grow, CAWI, N = 1000.

Polish fraud trends during the crisis

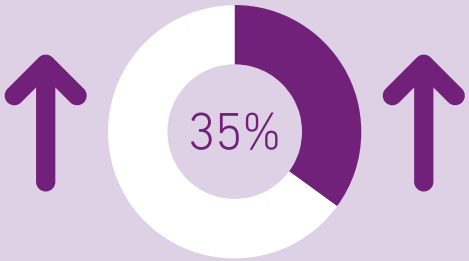
Anti-Fraud Platform

BIK is operating an Anti-Fraud Platform based on Experian's Hunter II system. Since its start it has protected the banking sector from frauds of the amount of PLN 252 million (updated on 30.06.2020).

PLN 252 million protected

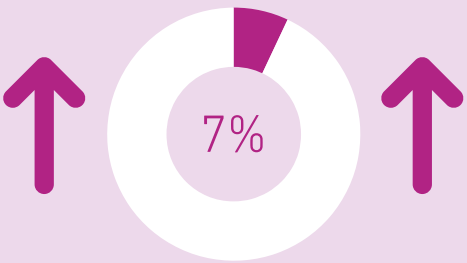
Fraud detection

Comparing the two pre-pandemic months (January and February 2020) to the early pandemic period - from March this year, the BIK Anti-Fraud Platform indicated a 35% increase in number of applications that was sent for verification in terms of detection of possible fraud attempts, while at the same time credit activity decreased due to the COVID-19 crisis.



Bank enquires

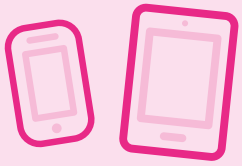
The number of inquiries increased by 7% about the Anti-Fraud Bank Report (BRA) addressed to BIK Anti-Fraud Platform by banks during the pandemic period – it proofs that during the COVID-19 crisis such a sectoral solution is becoming even more needed to reduce fraud losses as the financial institutions become more cautious and use the PAF system more frequently.



Fraud on devices

Obviously, business moved to online channels – the number of cases related to the electronic devices used by the client in the process of applying for credit are clearly confirmed by the CFD BIK Platform (The Cyber Fraud Detection Platform detects and analyses financial data and transactions through electronic devices).

The CFD Platform confirms an increase of 212% during the COVID-19 crisis of applying for credit products through online channels.



212% increase

Source: BIK S.A.

The road ahead

Obviously today, it is impossible to determine the duration of the current medical crisis. Nevertheless, first countries are attempting steps back to normal. But as expressed, it seems unlikely that criminal procedures, after recently peaking, will return to the lower levels experienced prior to the crisis.

Over the next few months, digital means for Fraud prevention will become a focus of attention. The fact that the identification of individuals, being a good customer or a criminal, is embedded digitally into the KYC processes by means of digital identity using digital biometrics, analytic and ML solutions is here to stay. Stolen clients' data will also remain available in the future.

Moreover, the substantial shift to digital business will be irreversible. Investments into digital means of fraud and risk mitigation, are mandatory for the crisis mode and will be necessary in the world after.

It is not a psychic prophesy, that consumers attention to digital risks will continue to rise. While this will further increase expectations to businesses to secure their systems and communication channels, it also brings new business opportunities as the security of identity is raising alongside these developments.

Early movers will shape the market in their favor

Whilst the globalisation of crime was a reality before the current crisis, it has recently seen unprecedented highs. This is a development that is here to stay.

Only prevention methods that go beyond single corporations' data and insight, will prove effective – global Fraud schemes will be addressed most effectively by using global insight for the prevention.

Key take away from this paper

- **Keep Fraud Risk at the top of your agenda,** it will be "back" soon
- **Digital is there to stay**, especially in regards to Fraud
- **The definition of identity changed** – it changed from personal data only and added digital identity
- **Flexibility of your Fraud prevention capabilities is key** in your Fraud Management setup
  - Experian offers holistic and flexible Fraud prevention solutions
  - Combination of software and analytics are the road to success
- **Your client's identity is at risk** – there is technology to keep it safe (and is a new revenue opportunity for your company)

Authors

Christof Seifert
Senior Fraud Consulant at Experian

Christof has over 20 years of experience in Credit Risk Management domain, with a special focus on the topics fraud prevention and collection management.

In 2014 he joined Experian – he leverages on his experience to help our customers to develop Anti-Fraud strategies and the implementation of Anti-Fraud IT solutions.

Bartosz Wójcicki
Director, Anti-Fraud Services Bureau, BIK

Bartosz is a graduate of the Warsaw University of Technology, Faculty of Electronics and Information Technology. He has over 10 years of experience in the area of counteracting crimes related to banking activities. When he was working in the banking sector, he was responsible for operational risk management, including crime prevention, compliance risk and AML. He has experience related to the protection of personal data and the protection of persons and property. From 2014, he was responsible for the development of anti-fraud products offered by BIK SA.

Iga Sikorska
Senior Analytics Consultant, CEE DACH at Experian

PhD-level professional recognised for sound knowledge of data science and effective communication across disciplines and management levels. Fraud Prevention and Detection expert with proven ability to understand customer business needs, identify alternatives, and recommend strategies that facilitate optimal and creative outcomes. Regional data science expert in fraud initiatives for banking and financial institutions supporting customers in developing analytically-driven solutions designed to innovate and optimise operational and business processes with a think outside of the box twist. On a daily basis, cooperating with global R&D in developing innovative, industry leading solutions for fraud prevention facilitating automated decisioning and quick investigation.

Experian Polska
Metropolitan Complex
Plac Pilsudskiego 3
00-078 Warsaw, Poland

T: +48 22 449 0119
www.experian.com.pl

C-00631