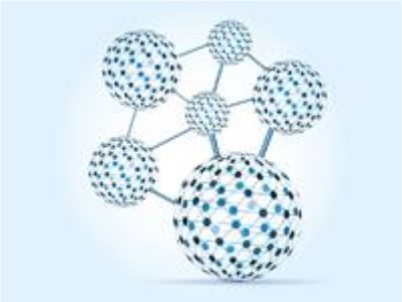
www.pipelinepub.com
Volume 17, Issue 1

Combatting COVID Fraud Risks

By: Stu Bradley, Sundeep Tengur



The telecommunications industry, much like its banking and financial services counterparts, is amid a period of turmoil. The impacts of the novel coronavirus have led to an economic downturn, which experts anticipate will have greater impacts than 2008's financial crisis. Arson attacks on 5G masts have grabbed headlines, but less visible fraud attacks on communications service providers (CSPs) have potential for more significant long-term damage.

Airtime abuse, subscription fraud, and other schemes cost CSPs an estimated $28.3 billion worldwide in 2019, according to the Communications Fraud Control Association. Fraud losses directly impact bottom lines such that CSPs can no longer sustain nor absorb these losses as a cost of doing business. It's past time for industry leaders to gain an edge on this growing problem, now exacerbated by the pandemic.

Enemies at the door

The telecommunications industry has always had to contend with opportunistic fraud—and with much of the economy on hold, organized fraud rings are intensifying their assaults. Fraud ring leaders understand the industry's current detection strategies remain mostly reactive. They devise modes to circumvent existing fraud barriers and slip through the cracks with relative ease. Among their favored strategies, fraudsters extensively use stolen or fabricated identities to access valuable smartphones and services. They also employ "mules"—typically individuals lured by easy cash—to visit stores and obtain as many post-paid smartphones as possible.

Facing criminals' increased velocity and sophistication, CSPs have no choice but to move their fraud prevention mechanisms upstream. The traditional find-a-needle-in-a-haystack detection approach has proven too complex, time-consuming and costly. It's far better to keep the bad actors off the books from the outset.

According to the Technology Research Institute, “Real-time point-of-sale identity verification services are invaluable to stopping fraudsters from exploiting identity theft." CSPs can gain an edge over their attackers by using a combination of entity resolution, peer group profiling, and risk scoring on both internal and third-party data (e.g., credit bureau, device profiling, geolocation, and other data).

Identity is the new gold

Data privacy and identity authentication will be a key priority for CSPs in their ongoing fight against fraud. COVID-19 has pushed many consumers and businesses online, and a large and growing number rely on telecommunication services to transact. But even as they embrace new means for transacting, many fear the unauthorized use of their data and the financial losses that may result—and for good reason.

At least 7.9 billion highly sensitive, personal records were exposed through data breaches in 2019 alone. The commoditization of this data on the dark web makes it easier than ever for nefarious individuals and crime rings to steal identities—and even concoct convincing fake ones.

The industry must prioritize the ability to authenticate and verify digital identity in a frictionless, non-intrusive manner. These capabilities will not only help reduce account takeover scams like SIM swaps, but they also boost the customer experience—a critical differentiator in a competitive market.

Revamped governance

Navigating work-from-home orders and social distancing measures, many CSPs are doing business outside their typical operational framework. For example, while most organizations have on-premise solutions for fraud management, investigations and analysis, investigators working from home may not have optimal access to the data and systems. Such factors can increase fraud losses.

Many mobile network operators (MNOs) recognize such losses are no longer sustainable, particularly when added to costs associated with local and international regulatory compliance and ongoing efforts around brand reputation preservation. It is therefore essential that CSPs appoint dedicated leaders accountable for a robust fraud strategy. These leaders should ideally have a direct reporting line to the C-level to ensure that fraud is factored into the company’s business continuity plan during and after the pandemic.

Telecom operators must also understand they cannot win this fight alone. Customer awareness is critical to fighting fraud schemes. Similar to hand hygiene and social distancing guidelines enacted to curb the spread of COVID-19, CSPs must educate their customers to recognize the often subtle signs of fraud— particularly now as schemers are using COVID scams to lure unsuspecting victims into their traps.

Optimize and automate

The current state of play forces businesses to adapt to pandemic-driven change. Priorities must be redefined and resources reallocated to high-risk and mission-critical tasks. Operational workstreams must likewise evolve to reflect the new “normal.” For example, as travel restrictions remain in effect throughout the world, CSPs must consider once ordinary instances of roaming as potentially suspicious events. But with roaming fraud tamped down, criminal networks will only shift to other methods, like Wangiri (Japanese for "one ring and drop") ploys to generate funds through socially engineered call-backs to premium rate numbers.

Using analytical techniques such as real-time peer group analysis, watchlist monitoring and anomaly detection, CSPs can be proactive and prepared to quickly lock down risky high termination rate numbers tied to such International Revenue Share Fraud (IRSF) schemes.

Make artificial intelligence (AI) the core

Today’s public health crisis is a stark reminder of the fragility of our health and economic business models. It’s not enough to merely navigate the current crisis. We have an obligation to be better equipped to respond to future "black swan” events. Businesses have the power of big data, technology and advanced analytics on their side, and they should look beyond digital transformation to adopt AI at the core of their operational frameworks.

AI can be trained to do the heavy lifting and, once tuned, deliver operational benefits such as optimized alert workload and improved scoring and decisioning effectiveness for better detection rates. AI can also reduce time to market for new offerings and help reallocate manpower from routine operations to more value-added tasks. These improvements help drive down costs, making them well worth the investment.

Operationalizing AI

While AI has the power to reinvent how we do business, many operational teams still perceive it as a black box and struggle with that concern. While it’s true that some models and techniques are inherently more opaque than others, AI can (and should) be engineered with “explainability” to foster trust.

Understanding the logic and reasons behind a risk score leads to greater acceptance of AI, which in turn can help businesses to better handle customer objections and deliver better service. It also deters employees from bypassing risk scoring to achieve a desired outcome for the client. In short, trusting the outcome of the AI model can help enforce operational governance and achieve enterprise excellence.

For AI to be explainable, it’s critical that CSPs are involved in the modelling process and “own” their AI strategy. Failing to do so is akin to sailing a ship without a captain. Business leaders do not need an AI strategy; rather, they need AI to *be* their strategy.

The telcos of tomorrow

The pandemic has highlighted the paramount role CSPs will continue to play in connecting people and business. However, beyond-the-business as usual operations, most telcos strive to tap into new markets. For many CSPs, mobile wallets are already standard offerings, primarily in emerging economies. In the EU, for example, market changes and new regulations such as PSD2 (Payments Services Directive) are propelling telcos to push into the payments and financial services space. In the US, many technology, media, and telecommunications (TMT) companies are maneuvering to acquire a bigger share of the gaming and streaming market.

From a strategic perspective, the pandemic is certainly a setback. But it also presents a tremendous opportunity for the industry and individual providers to leap forward. CSPs with the right blend of capabilities and a willingness to adapt will have a significant advantage.

Expect and prepare for the unexpected

COVID-19 has taught the world some valuable lessons, among them that we must be better prepared to deal with so-called black swans. Although uncommon, unexpected events are prevalent across all industries, and in our fast paced, more-connected-than-ever world, they will tend to occur more frequently and have farther-reaching impacts.

With globalization, and as CSPs continue to expand their service offerings, risks will follow. The CSPs that survive and thrive will be the ones that are adaptable and able to turn risks into opportunities. Importantly, organizations can reduce and better manage the ill effects of unexpected events using the power of analytics. Though techniques like anomaly detection and predictive analytics have existed for many years, today's commoditized computational power and readily available big data allow anti-fraud technology to soar to its full potential. Advanced analytics can help stop fraud, even *before* it happens.

While the industry remains uniquely focused on criminal activity through the lens of the pandemic, fraud is an ever-present and growing issue that demands attention. Whatever the future holds, telcos that pivot to treat fraud as a strategic issue and use advanced analytics to augment and refocus their fraud fighting efforts will be best positioned to act quickly against changing threats.