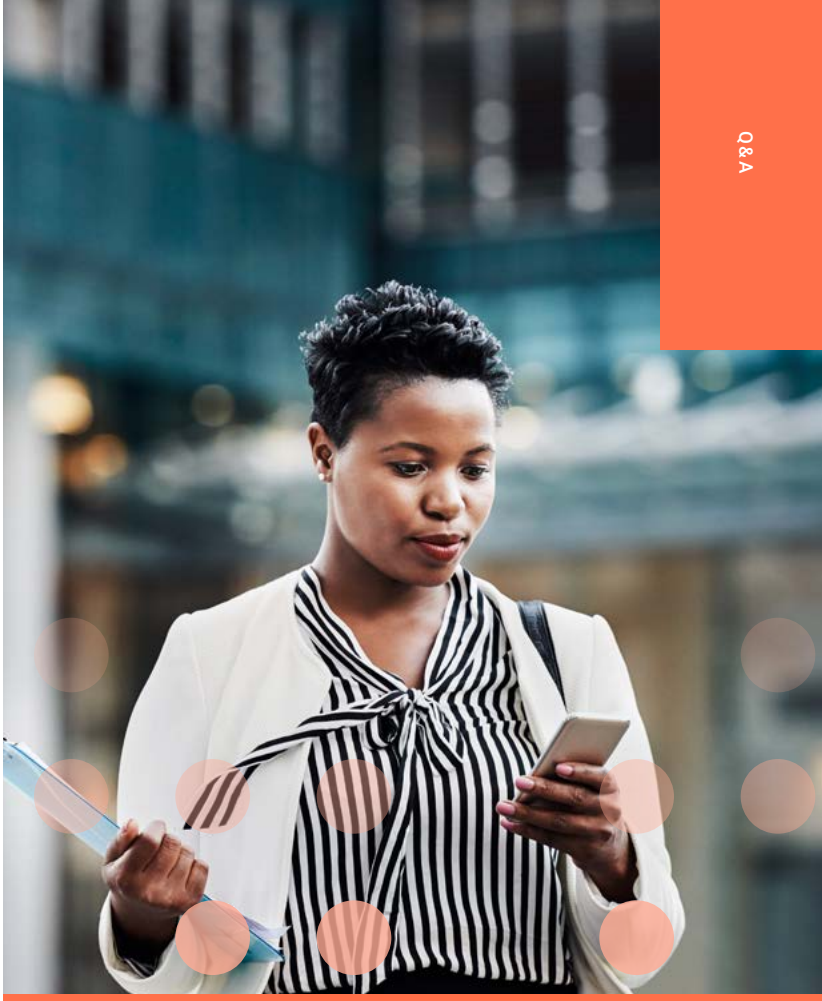
Fraud Protection & Compliance
Telecommunications

Q&A

Applying Predictive Analytics in Telecommunications to Stop Money Laundering



Anat Hoida

Head of FICO EMEA Telecom Practice

The telecommunications industry provides essential services for businesses and consumers alike. As enterprises, products, and industries become increasingly digitalized, the internet and mobile service networks have become ubiquitous. One consequence of this is that the line between telecommunications and financial services is starting to blur in some areas. Mobile devices are expensive, and communications service providers (CSPs) increasingly are involved in financing them for customers. Meanwhile, CSPs have begun offering platforms for financial services, such as mobile money and microlending services in emerging markets. While these trends represent major opportunities for CSPs, they also bring with them new compliance requirements and regulatory hurdles.

FICO

CSPs now share with financial service companies the same responsibility to prevent the use of their infrastructures to perpetrate financial crimes, especially money laundering. Once they provide financial services, CSPs must implement anti-money laundering (AML) measures, and see to it that their networks are not being used by individuals or organizations who are known criminals or terrorists. CSPs are also responsible for seeing to it that their customers who are listed on international registers of high-risk individuals are subjected to due diligence—at account origination and over the lifecycle of the relationship. These duties can consume technical resources and administrative overhead costs. For small institutions, the financial burden can be significant.

In this conversation, Anat Hoida, head of the EMEA Telecom Practice at FICO, explains how the telecom industry is evolving and how automation, including increasingly powerful analytics, is helping CSPs absorb their new responsibilities in fighting financial crime.

Q:
Some telecommunications providers are adopting business models that look increasingly like those of financial service companies. Is this driving interest among CSPs in anti-financial crime measures?

A:
From a regulatory perspective, as soon as you start to provide financial services, you have to have a compliance solution in place, and you have to report to the authorities any evidence of money laundering. You are also required to prove that you are not providing service to anyone who is sanctioned under anti-money laundering law. Failure to prove so can result in a massive fine, and the liability associated with this is not only to the organization but to individuals—typically the CFO or chief compliance officer, and potentially to others who were involved. The regulators will insist that individuals take personal responsibility for their actions.

Q:
Before CSPs got involved in financial services, was there a concern that a phone or the account might be seen as a medium for money laundering?

A:
Prepaid accounts have sometimes been used that way. At least in the UK, a CSP that is not providing financial services is not regulated by the Financial Conduct Authority or other regulators of financial services, and therefore not obliged to have a compliance solution in place to detect financial crime. But those who provide financial services are now subject to regulation. It's not that the problem wasn't there before; they just weren't required by law to have the solution in place.

Financial services include the direct financing of handsets, credit cards, and mobile money services. As soon as you move away from the subsidy model, you are effectively providing financial services.

In Germany, currently, CSPs are not financing these devices. They use the subsidy model, and what they provide to customers is not considered a loan, so the telecoms are not subject to the same financial regulation. But the Germans want iPhones and other expensive devices just as everyone else does, so over time it's likely they will evolve a financing model as well. We have seen this shift originally in the US and gradually shifting into Europe. In some European countries, this is driven via the telecom regulator or the consumer protection office, which is responsible for safeguarding the individuals from overpaying for their service.

CSPs will start to provide financial services, and therefore come under financial regulation, when they have to. In the US, the "big four" all finance their equipment. In EMEA, that's not the case. It's a shift that's taking place gradually, and it's not always because of handset financing. A CSP might decide to create its own credit card. As soon as they do, they will need to have a financial crime solution in place.

Generally speaking, they should know this. They need at very least a Know Your Customer (KYC) solution to prove that they are not providing service to sanctioned individuals and that if they are dealing with any Politically Exposed Persons (PEPs), those individuals are treated with due diligence.

They should have measures in place to prevent money laundering, and a system for monitoring accounts over time—what kind of monitoring depends on what financial services they offer. And the requirements would vary from country to country.

Q:
There are examples of CSPs actually providing banking services, right?

A:
Yes. It's increasingly common in markets like Africa, where mobile money applications provide an important source of micro loans. Each loan is a small amount of money, but the provider is still required to check for suspicious patterns of activity.

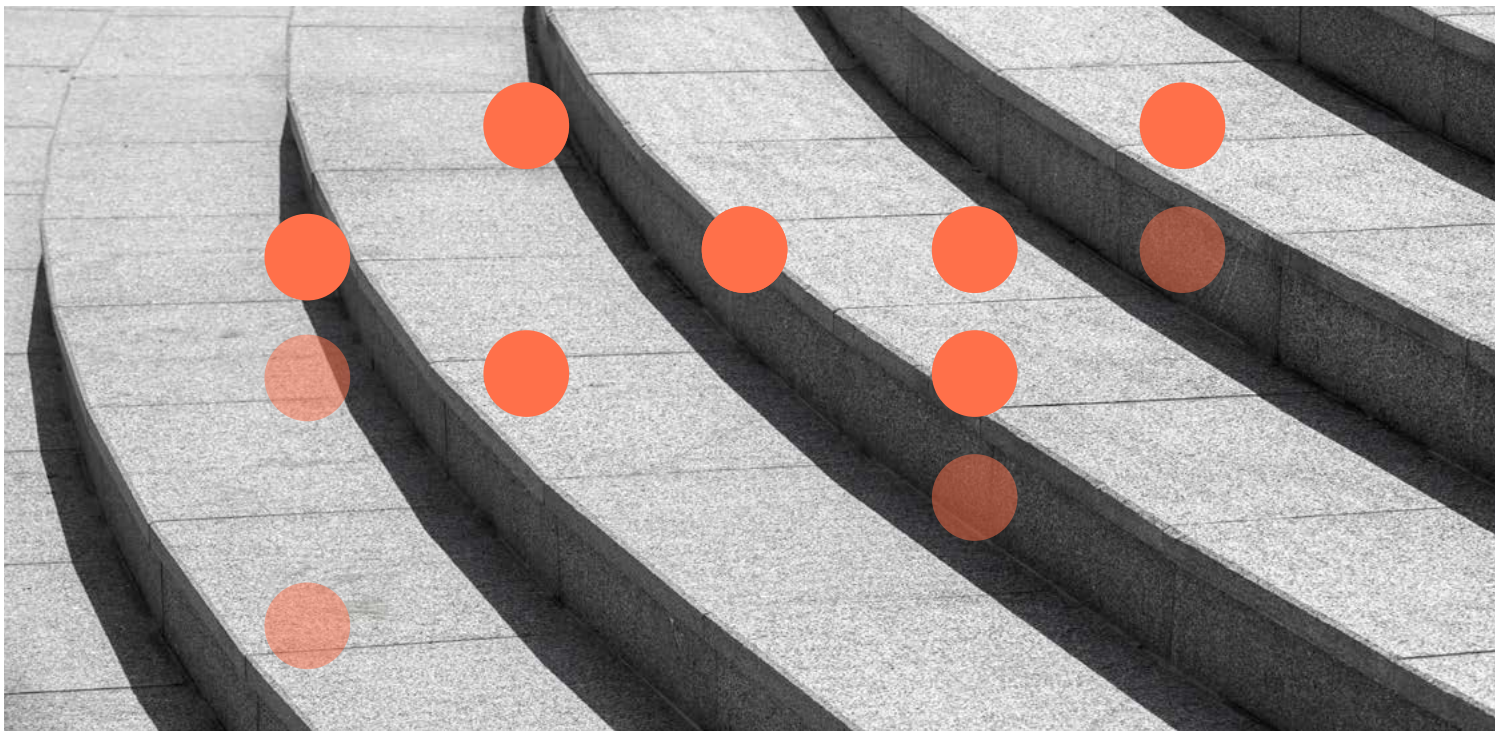
FICO's technology can help in two ways. It can be used to track the movement of funds, looking for patterns that might indicate the financing of illicit activity. But the first line of defense is the KYC piece. Mobile money providers need to identify who their customer is to make sure that customer is not listed on one of the watch lists maintained by the US, the EU, or the Bank of England.

Q:
How does FICO address financial crime?

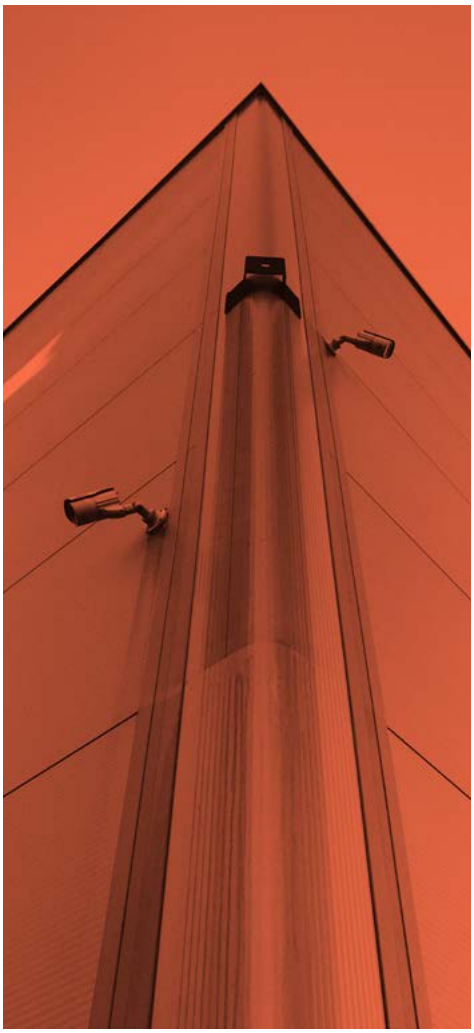
A:

The big picture for financial crime includes fraud, an application where FICO® Falcon® technology has been important for decades. But FICO is an important player in KYC and anti-money laundering as well. In 2015, FICO acquired a company called TONBELLER, which has been in the anti-money laundering space for about two decades and provides advanced technology. The merger gives FICO a more holistic view of financial crime.

The TONBELLER solution, called Siron®, is live at more than 1,200 customers around the world. It can be used by any kind of financial institution, small, medium, or large, including retail banking, private banking, domestic or multinational, and more recently it has been adopted in telecom. Siron has multiple modules, and transaction monitoring for AML is just one of them.



Q:
Fraud detection is often closely associated with anti-money laundering and KYC. Do these challenges lend themselves to the same technical approach?



A:

Basically, yes. When a CSP becomes a victim, it loses money because it becomes responsible for the loss. But what may count even more is the damage to the company's reputation. There have been many accounts in the press of money laundering scandals, including incidents involving some of Europe's biggest financial institutions. Companies need to avoid this negative reputational impact.

A FICO engagement usually begins with a business risk assessment, to help a telecom provider understand what might happen, based on the products they are offering, the customers and geographies they are operating in. We will generate a risk heat map to provide a full picture of the risks related to money laundering, and explain the approach we will take to mitigating these risks. It's important to understand the situation first.

KYC becomes the first line of defense. We capture customer data, screen it against third-party watch lists, including identification of people who, because of their positions, might be exposed to corrupt political activity. By definition, any politician is a high-risk customer, along with his or her family. Large or high-profile donors to political campaigns are considered politically exposed.

There are the Dow Jones Watchlist, World-Check, LEXIS-NEXIS, and other databases containing information on 2 million politicians and other politically exposed persons that we can screen against. There are similar terrorist lists. The outcome of KYC will be a risk classification for each customer—a high, medium, or low risk customer. For a high-risk customer, you are supposed to perform an enhanced due diligence check. For a low-risk customer, the law allows you to perform simplified due diligence. Enhanced due diligence means intense money laundering checks; simplified due diligence means very basic checks.

This is all defined by law—in the US, for example, by the USA Patriot Act. After the risk classification, and after onboarding, the customer will start executing transactions. Those transactions are tracked using our transaction monitoring component, Siron AML, to look for anomalies, unusual behaviors, and those that trigger money laundering alerts. An AML investigator can look at those alerts and make decisions. Either the situation can be explained by normal behavior or it cannot. If necessary, the investigator will file a suspicious activity report. This is a regulatory filing that allows the CSP to avoid the reputational damage from a money laundering incident. The regulatory filing is managed by our alert and case management module, Siron ACM.

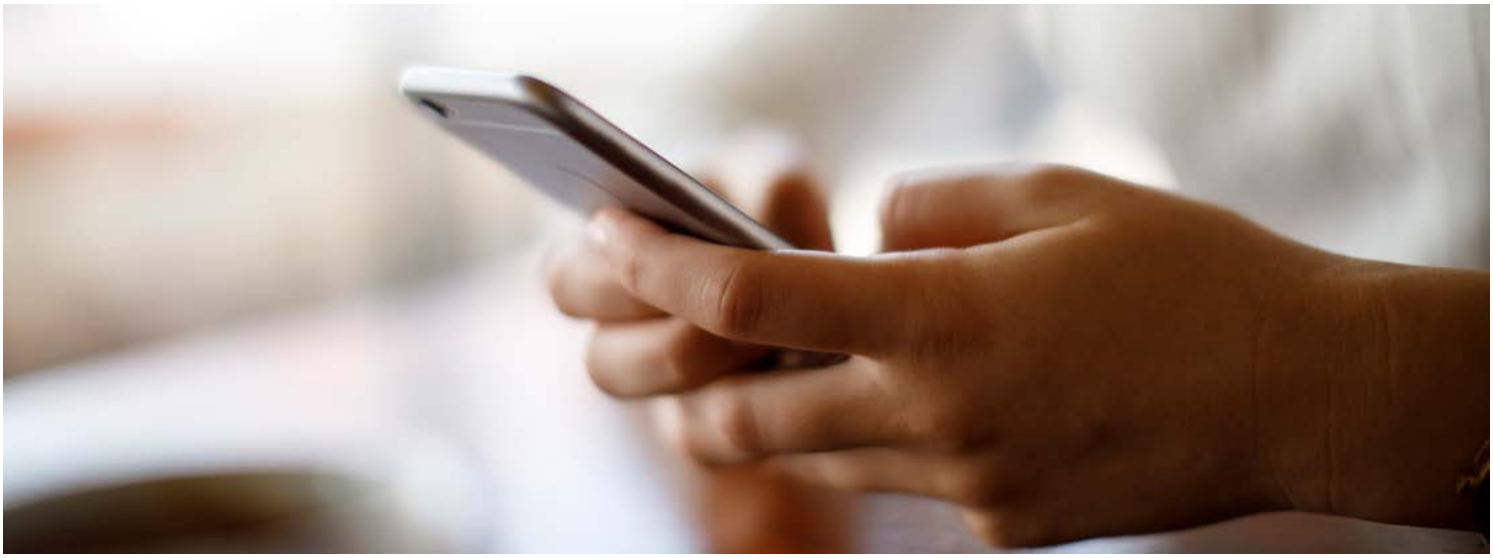
Notice that we are not the data provider. We rely on third-party data. The transaction screening is not just at the point of onboarding, it's a continuous process and an individual's risk classification may change over time. The customer may have no matches to any data in the public databases, so at onboarding, he will be subjected only to simplified due diligence. But over time, his profile may change if the system notes suspicious patterns of activity in his account. For example, he may start wiring money to high-risk countries, or the behavior in the account will not match up with the customer's KYC profile.

Machine learning can spot these anomalies. The customer will be reclassified as higher-risk, and will be subjected to greater due diligence.

Q:
Does due diligence only apply to individuals?

A:

No. In telecom, it is very important to examine the beneficial owners of corporate customers—who stands behind the company? We can do KYC checks against Dun & Bradstreet, Bureau Van Dyck, and other databases. We can detect changes in beneficial ownership, and the new owners can be checked against the politically exposed persons databases. If we get a hit, the system will automatically classify the company as higher-risk. That's part of FICO's KYC lifecycle support. It's out-of-the-box functionality.



Q:
Crime networks come and go as situations change. Whose responsibility is it to know who is a high-risk individual?

A:

It's the responsibility of the lender or in this case, the CSP. If there is a problem and it becomes public, the compliance officer is the first person who is in trouble. Small banks have been shut down for failing to recognize that their accounts were being misused for money laundering or terrorism financing. For a very large CSP that is providing financially oriented services, the regulatory risk can be quite significant.

If a customer turns up as high-risk in a money laundering or terrorism financing database, the CSP is not allowed to do any further business with that individual, and the system's transaction screening will block any further transactions and suggest terminating the customer relationship.

Q:
It sounds as though the technology underlying fraud detection, AML, and KYC is fairly similar.

A:
It is. One of the most important things these use cases have in common is the risk classification. It will be fed by rules, predictive models, and AI. Those are important enablers, but from a business perspective, the critical thing to understand is the risk classification; once you have this, the next steps to mitigate become much clearer.

To learn more about FICO, visit www.fico.com

4736EX 07/19 PDF

FOR MORE INFORMATION
www.fico.com
www.fico.com/blogs

NORTH AMERICA
+1 888 342 6336
info@fico.com

LATIN AMERICA & CARIBBEAN
+55 11 5189 8267
LAC_info@fico.com

EUROPE, MIDDLE EAST & AFRICA
+44 (0) 207 940 8718
emeainfo@fico.com

ASIA PACIFIC
+65 6422 7700
infoasia@fico.com