As fraud evolves, banks will require newer techniques to combat losses

By Mohan Jayaraman, Managing Director, Experian Credit Bureau, India

An increasing number of digital transactions are being seen which move into the yet unregulated FinTech space. Banks continue to partner with these players for better customer experience, and at times the quality of safeguards is still a concern. Can this be controlled? Are banks developing a comprehensive risk management program that incorporates appropriate risk assessments of FinTech players?

Well, we end up having this discussion often. The world is getting to a place where open APIs (application programming interface) are becoming the name of the game. When you publish your APIs they are getting published in somebody else's chain. This no doubt is adding value to the customer. However, the consequence is that now there are more complexities associated with entry points and there are multiple things that can go wrong.

However, this may not be the part that needs to be controlled. I think what needs to happen is that financial players need to put in a lot of infrastructure in place to prevent frauds. The traditional mindset with banks has been that investments will be made as commensurate to the current scale of fraud or what is required. Banks have to be ready for the future. Given that the volumes in the country can increase anytime, and demonitisation has already tested the banks, they now need to invest for the many and not the few. The industry may still be in the mindset to prevent frauds for the few.

Beating the bad guys

Fraud management investment by banks is very conservative. Unfortunately, fraud management is an area that requires large investments. That's the point that should be continuously made to banks. The point is that the guys on the other side are spending ever increasing efforts, in a distributed manner to break into the banking system.

In the past, fraud was perpetrated by a couple of unemployed youths trying to make some quick money. Today it is an organized activity. There are sovereign efforts to create repositories that enable fraud.

In a specific instance, during the investigation of a fraud in a particular country, it was found that there were people employed full-time who were creating a database of users. They were like everyday professionals, and their

9 to 5 job was to collect user information and credentials, and sell it to those who commit or execute frauds. To fight such organisations businesses cannot use traditional methods.

Now, let’s look at the way UPI is growing. Transaction banking needs to have lot of fraud detection and prevention capabilities. When we use an e-wallet today, most of us don’t link our credit card details to it. Why? Because we are not sure if we are completely secure. There is this fear. This fear needs to go away.

Everyone needs to understand how fraud is evolving as a science. Earlier it was only about stealing a person’s credentials. The first big growth wave in fraud happened when there was division of labor between data collection and actual fraud perpetration. So businesses, provided insulation to a certain set of people who were carrying out data collection. But now, because the two have been insulated, there is an ability to grow it. That’s providing the scale. The second big thing that’s happening is proliferation of entry points. Earlier there were a limited number of computers/connections.

Now with mobile penetration and huge growth; device level fraud detection and protection is starting to become contextually much more important. That’s the next wave which can become more important in the Indian context. You can’t protect a network but what you can do is create a whitelist of devices or access points and equally create a blacklist and have shades in between where one might need to probe and get more details on the authenticity of devices.