Payments Fraud

The Rise of Digitalization is Changing the Payments Industry

Global payments are expected to exceed $2.3 trillion by 2019, and each year, with non-cash payments accounting for an increasing share of this massive market. Cashless transactions are growing by 10%, and according to one source, are likely to represent over one million transactions every minute by 2020. The increase is mainly driven by accelerated growth in developing markets, primarily driven by digitization and alternate channels.

Although cards remain the dominant and fastest growing payment instrument, the landscape is poised for rapid change and market disruption. The growing adoption of mobile payments, particularly among millennials, combined with a rapid uptake in e-commerce "Card Not Present" (CNP) transactions, and the emergence of non-banking payment service providers (FinTech) are among the many factors causing turbulence and disintermediation in discrete parts of banking and the payments landscape. According to US Census Bureau, US e-commerce transactions grew by 15% in 2016.

Digital payments which can be executed anywhere, anytime, from any device is naturally appealing to both buyers and sellers. The advantages, however, are accompanied by additional aspects, most notably fraud and theft. An estimated 73%[3] of enterprises report some form of suspicious activity that puts around $7.6 of every $100 transacted at risk.

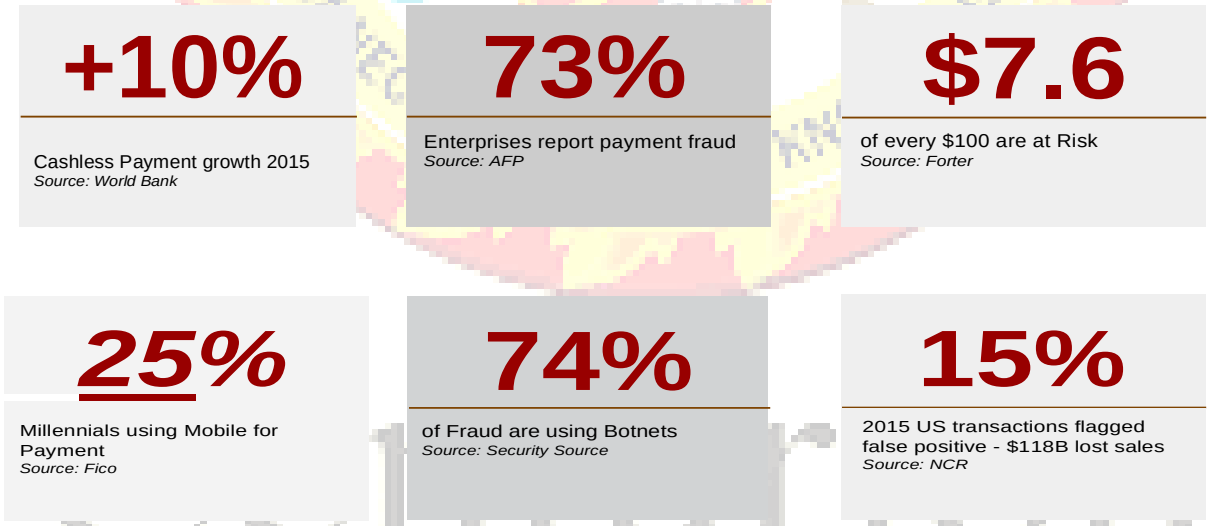

Figure 1: Digitalization in Payments Leads to Fraud

Forces of Change that Drive Fraud

The payments industry has historically been relatively insulated from disruption. An extensive web of laws and regulations, combined with high capital barriers to entry, have limited the number of industry participants and fostered decades of relative stability. This is changing. A confluence of trends in technology, business, the global regulatory environment, and consumer behavioral patterns are redefining how payment transactions are executed.

One fundamental aspect of digitalization is the increased adoption of online and mobile channels that has been a boon for perpetrators of fraud. According to Forrester, there has been 62% increase in payment fraud since Oct 2015. These channels triggers increased number of false positives (i.e.: legitimate transactions being denied) and is estimated to have an economic impact of $188B during 2015 in US alone.

The increased touch points and the nature of those channels lends itself nicely to fraud by masking and hijacking the identity of the mobile user. Consumers are propelling the digital payments industry in all facets of everyday life — ride sharing, digital music, movie tickets, vacation rentals, and online auctions represent just a few of the generators of digital payments. Their expectations now demand more seamless and hybrid experiences, like combining commerce with payment, payment with social etc. At the same time regulations are forcing some rule-leveling barriers and access to the consumer data is becoming democratized. This democratization of access and information means there could be more leaky faucets and a lot of them are non-traditional payment players.

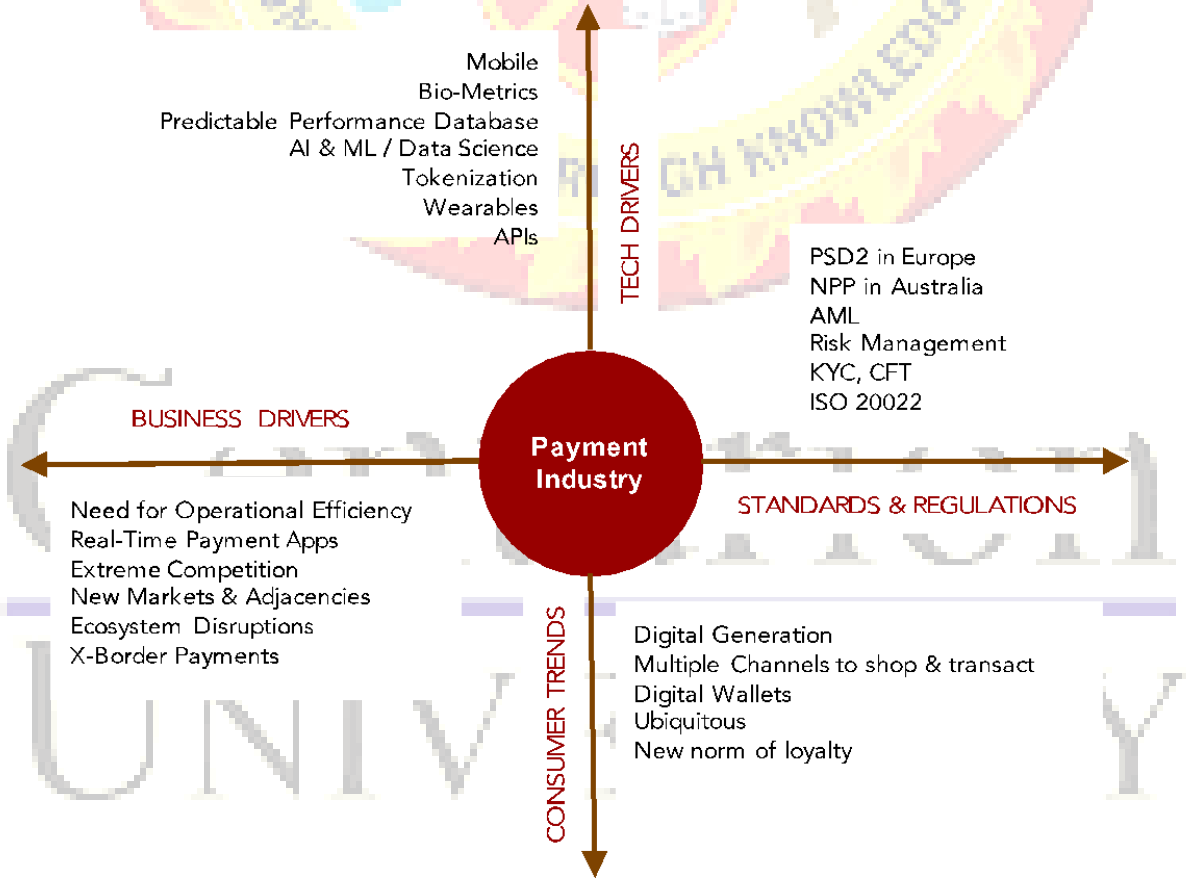

Figure 2: Confluence of Forces

All of these factors bring in unique, non-traditional attack patterns. One such mechanism is DDOS (distributed denial of service) style attacks where multiple affected systems initiate a fraud activity in a very short amount of time within a threshold to avoid detection. Another specific impact is CNP (Card-not-present) fraud. Migration of card payments from magnetic stripes to EMV Chip and PIN is witnessing a simultaneous shift in fraudulent activity from the card presented to the CNP category. As EMV (chip) becomes mandatory in card transactions, most fraudsters are going online and, in 2016, the CNP fraud rose between 12-15% over the previous year.

Fraudsters now coordinate fraud schemes across all transaction channels and use a wide array of tools to attack:

- Device compromise (means of actively altering the state of a device to compromise it on security and quality)
- MitM attacks (secretly altering communication between 2 trusted parties)
- Spoofing (sending fraudulent communication from an unknown source disguised as a legitimate source)
- Botnets (using a network of infected computers to initiate fraud transactions)
- Location Manipulation (manipulating the actual location of a device or transaction)

According to Secure Source, 74% of Payment fraud that originated last year were through Botnets. As digitization starts to encourage non-traditional players, payment service providers are looking at ways to deter fraud, reduce risk and create value.

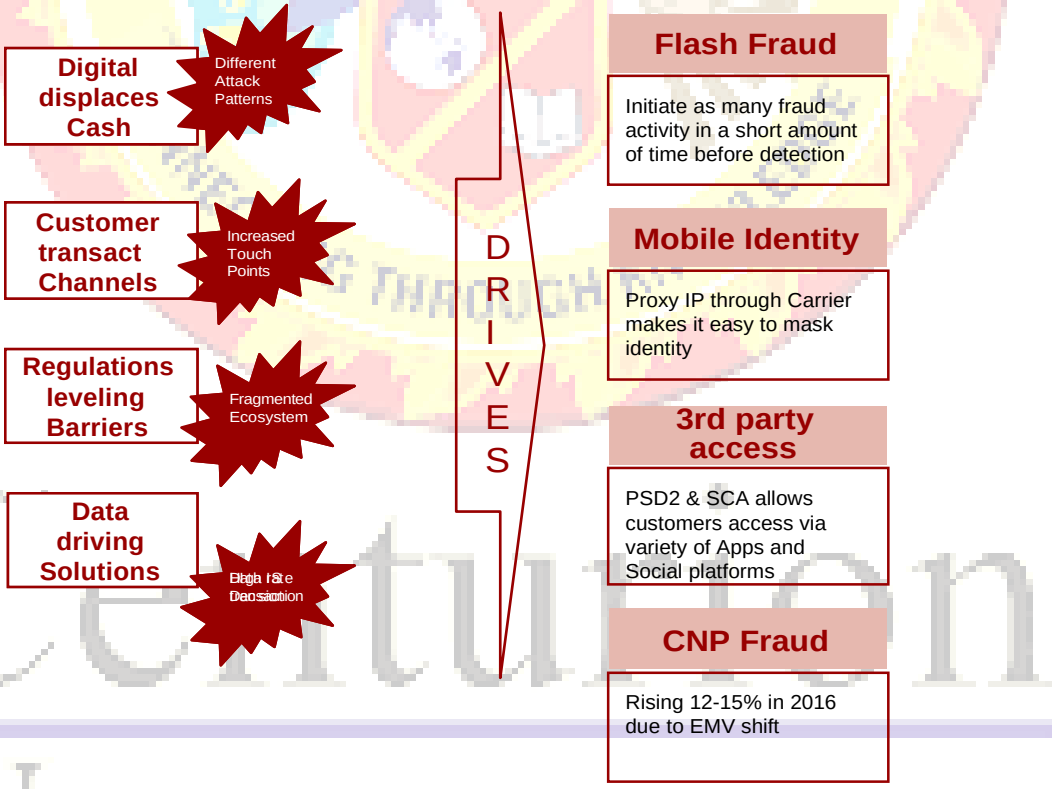

Figure 3: Payment Fraud Drivers

Signature of Fraud Prevention

Fraud is costly. It kills loyalty. Banks, credit card companies, payment processors, money transfer firms and settlement vendors know the huge impact of fraud on the success of their business.

Fraudulent transactions can not only impact revenue, but also compromise user trust and lifetime value. Yet preventing fraud is a balancing act between identifying criminal behavior while minimizing friction for trusted users.

The way firms have been dealing with fraud has changed over the years (see Table1). The market today dictates that fraud detection and prevention be:

- Agnostic, to any kind of threat, whether it is a botnet, or a location manipulation, or a lost device
- Omni-channel, and support detections and actions across all forms of consumer interactions
- Dynamic, using real-time scoring of risk patterns and specific to a particular transaction for a particular device and particular consumer for a particular event
- Contextual, using many different data and signatures to come up with a unique assessment of risk
- Fast and real-time, within the boundary of application transaction. e.g.: if a consumer is swiping a card, the entire fraud check should be done in milliseconds within the limit of the commerce transaction.

Characteristics	Old way	New way
Type of Threat	Mostly threat specific (e.g.: Stolen cards, or DDOS)	Threat agnostic (e.g.: real-time fraud actions)
Type of Channel	Single channel to holistic, limited to an application or pools of them (wire transfer, ACH etc.)	Omni-channel transacting across Mobile, Online and Physical worlds
Analytics process	from basic rule-mapping to getting a few data points beyond a typical user interaction	Dynamic, real-time risk scoring, analyze per consumer/per device/per channel/per transaction
Transactions	Transaction centric (manual and some pattern matching to drive decisions)	Contextual (unique customer signature from application, bureau, derived-value & cross-product data at account, customer, product and network level)
Speed	Batch and micro-batch	Real-time decisions at edge closer to data

Table 1: Fraud characteristics over the years

Fraud detection and prevention therefore hinges on consuming large volumes of data, analyzing and discovering patterns and driving decisions in real-time. These decisions can be based on a multitude of factors and can be an amalgamation of many micro-decisions.

Managing Tomorrow's Fraud Through Systems of Engagement

Fraud systems rely on many "micro-decisions" at every touch point to make an accurate assessment of potential fraud and formulate a complete risk profile.
These decisions are based broadly on

- Knowing the customer, based on real-time synthesis of data - social, demographics, purchases, preferences, etc.
- Monitoring transactions across the broader cyber space and across every available channel.
- Analyzing the patterns in real-time.

Figure 4: Fraud Prevention Continuum

Specifically, these systems:

1. Ingest data from customers that is specific to the channel and enables firms to define specific policies, rules, and algorithms associated with that channel. E.G.: if a user typically signs in via a different mobile OS device or the user typically makes a payment every month but the past two transactions happened days apart, the platform should not make quick rule based judgments on a single pattern but make many micro-decisions across many elements and formulate a risk score.

2. Gather details from mobile devices, including geolocation and device information, and combine those details with the profile of the card, account holder, and device in order to assess the risk of a transaction in real time.

3. Drive Risk decisioning rules based on IP address, browser, fingerprint data, location identifiers, and device fingerprints

4. Actively Monitor card-not-present (CNP) and other digital interactions and transactions, and use intelligence from the various devices in conjunction with transactional data such as shopping cart information, payment information, billing and shipping information, loyalty information, and product details.

5. Formulate a behavioral profile based on geolocation, device profiling, trust scores based on merchant activity, customer engagement with real-time alerting and notification, social network analysis, and link analysis

Hence, payment fraud needs to be managed in a continuum – consisting of detection, prevention, and recovery – in a way that allows for integration and customization of products and services based on the needs of individual customers.

For electronic payments fraud prevention strategies to be successful, the processes must be tightly integrated with transaction processing systems. This integration enables real-time interdiction, and drives actions that are called automatically, based on policy. Automated systems can provide a more comprehensive view of customer behavior by leveraging analytic calculations and algorithms to detect and flag suspicious payments activity. Furthermore, these capabilities deliver very low false positives.

Figure 5: Payments Systems of Engagement

Limitations of Conventional Payment Fraud Analytics Systems

The modern payments value chain is long and complex, with data flowing back and forth continuously. This data is living and ever-changing but locked in silos.

Conventional Fraud Analytics architecture systems are built on systems of record and designed to analyze large volumes of historical data to produce fraud insights and predictions.

Conventional fraud analytics systems are siloed and not designed to keep up with the wide array of attacks on data and data sources. Many institutions perform manual reviews of transactions prior to initiation, an approach that is laborious, not scalable, and significantly more error-prone than an automated strategy. The wide range of access points for financial information and activity gives fraudsters an array of options to plan and execute their attack.

To keep up with this rapidly growing threat, payment providers must evolve from the traditional, siloed method of fraud detection to a proactive, analytic approach: the models were trained on historical data, frozen, then weighted or adjusted in batches. This led to almost no co-operative learning and decision making.

Prevailing data architectures:

- store transactional and analytical data in separate silos,
- fail to bring transactional data together with historical data for analysis in real time, and,
- are batch oriented.

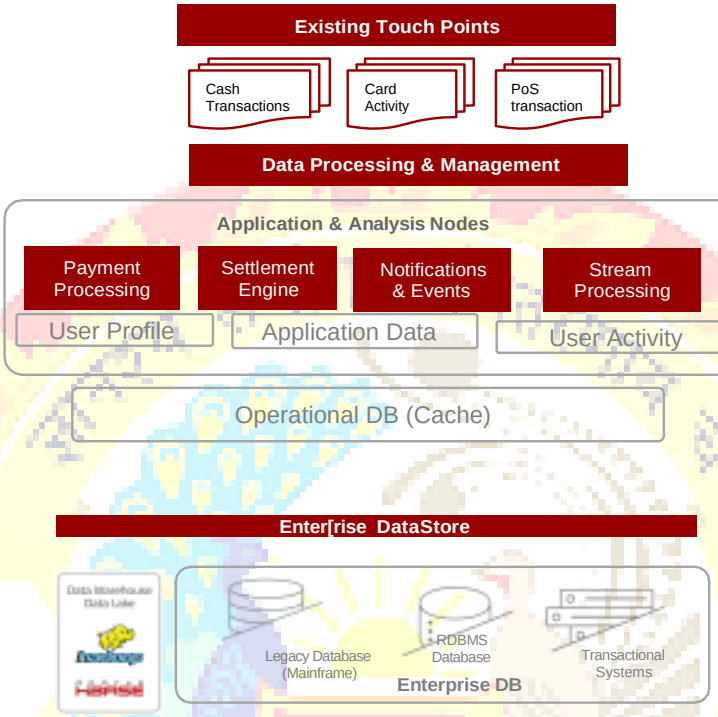

Figure 6: Conventional Payment Fraud analytics systems

They had an effect in their business outcomes:

- customer abandonment
- payment denial
- fraud
- missed cross-sell
- bad customer experience.

Learning Before "Approve-Flag-Block" in Milliseconds

Modern systems of engagement (SoEs) are incorporating a new generation of application architecture that eliminates the wall between transaction processing and analytics.

Many companies are now building transactional analytics systems for fraud to complement their existing architecture.

Gartner refers to this as "Hybrid Transaction/Analytical Processing" (HTAP). An HTAP architecture is best enabled by in-memory computing technology to enable analytical processing on the same (in memory) data store that is used to perform transaction processing.

By removing the latency associated with moving data from operational databases to data warehouses and data marts for analytical processing, this architecture enables real-time analytics and situation awareness on live transaction data.

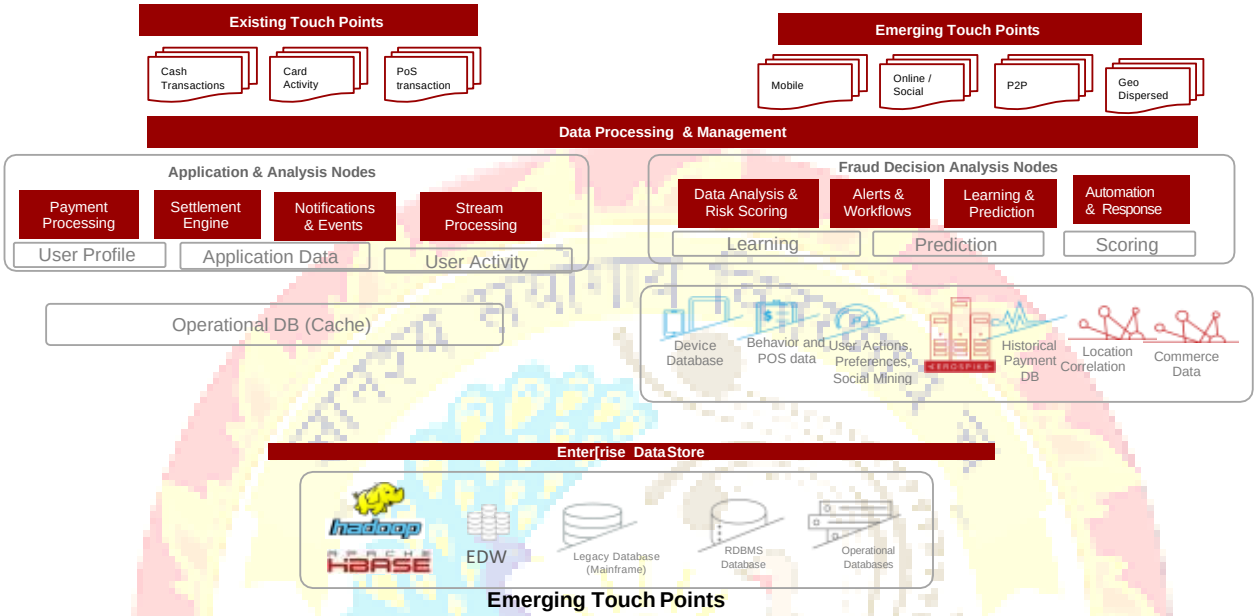

Figure 7: Payment Fraud Analytics of the Future

The key tenets of HTAP are:

- For real-time analytics within the scope of a single application or domain, data does not have to move from operational databases to data warehouses.
- Transactional data is readily available for analytics when created.
- Drill-down from analytic aggregates always points to fresh application data.
- HTAP reduces the need for multiple copies of the same data.

The ability to run analytics on live data and provide immediate feedback to the system is key to fraud deterrence.

Payment fraud solutions based on HTAP architecture generally consist of:

- Transaction risk-modeling, scoring, and rule-based elements that offer fraud alerts,
- An event management system, combined with data mining and reporting capabilities,
- Real-time fraud scoring based on advanced predictive and machine learning (ML) capabilities, and,
- Fast-acting, automated 2-way communication.

The amount of data that needs to be processed or learned from can be massive. The data could typically consist of: billions of historical payment data points; analysis of activity correlated to hundreds of millions of devices; behavior and device mismatch across a multitude of locations; user actions, preferences, and interactions; Geo policies, dependencies, and a myriad set of 3rd party information; Social and 3rd party consumer information; and, e-Commerce transactions.

It therefore is important to note that the efficiency and efficacy of the systems that prevent payment fraud depend on their power to harness data, analyze, learn it, and act upon it - with a very high accuracy rate and at near-instant speed.