Introduction
The introduction of EMV chip cards in 2015 led to expectations that fraud losses would fall. However, fraudsters proved they were ahead of the curve. US banks experienced more than $8.5 billion in fraud losses for payment cards in 2016, with those losses expected to surpass $12 billion by 2020.

Fraudsters have identified ways to adapt to new technologies. Traditionally, counterfeiting was the most common method fraudsters used to abuse the system. With the change in technology to EMV cards, it has become virtually impossible to copy a card. There has been a shift in fraud trends towards account takeovers (ATO) and fraudulent applications. With high-profile data compromises now making headlines on a consistent basis, customer personally identifiable information (PII) is now more easily available to cyber criminals. Many banks were unprepared for this change in the nature of fraud attacks.

Consumers continue to expect banks to protect them against fraud compromises and at the same time provide them with seamless experience and in this process two outcomes can occur. In the first, a company correctly identifies the fraud or potential for fraud. In the second, an account or transaction is falsely classified as fraudulent. In both cases, the potential benefit is limited to the amount of fraud dollars saved. The potential costs, however, go beyond the operations and plastic reissue cost. In the long run, the impact can be seen in customer attrition and low spending, lowering revenues for the bank. According to the 2016 ACI Worldwide Study of Consumers in 20 Countries, 53% of user card replacements are due to either fraud or data breaches. This shows the impact fraud can have on bank revenue in the long run, with 40% of consumers reducing their use of the replacement card after experiencing fraud.

Today, fraud organization leaders face the difficult task of mitigating fraud losses, balancing customer experience, and preparing their organizations for future. By seamlessly integrating analytics, operations, and technology, leaders can achieve their priorities and run a successful fraud risk organization.

Analytics
Though fraud only impacts only a fraction of one percent of all the purchases made with plastic, fraud losses are increasing even as fraud events are becoming rarer. Fraud’s dynamic nature makes it critically important that financial institutions leverage advanced analytics to mitigate fraud risk.

Leveraging analytics will require financial institutions to record all customer activity and maintain every bit of data generated, which can be analyzed to find the relevant data for preventing fraud. Financial institutions should capture data across customer lifecycle at several levels.

a. **Acquisition Level**: Data provided by customers and data from third-party sources like credit bureaus

b. **Transaction Level**: Customer interactions with the bank such as spend, payment, cash withdrawal, and other actions

c. **Digital/Non-Monetary**: Information about customer interactions with the bank via different channels

The true power of these different data sources can be realized by identifying the links between them, and combining these links with the right variables and features to identify fraudulent behavior. Once all the data sources can be leveraged, analytics can be used in two stages:

- **Monitoring**: Identifying problem areas and key loss drivers
- **Mitigation**: Using predictive analytics to target fraudulent activity
Monitoring

Monitoring helps identify any emerging fraud trends or potential attacks on the portfolio. It helps answer the question of whether things are going as they should, or if any outliers or anomalies have occurred. Millions of transactions happen each day, and identifying trends becomes dependent on the bank’s ability to channel, track, and act upon large amount of information.

A sound reporting system incorporating precise, trackable key performance indicators (KPIs) is essential to help business leaders make informed decisions.

Some important KPIs include:

- **Fraud Rate**: The percentage fraud transactions for a particular segment
- **Approval Rate**: The percentage of approved transactions within a particular segment
- **Decline Rate**: The percentage of declines within a particular segment
- **Coverage**: How many fraudulent transactions were detected
- **Authorizations**: The total number of authorizations posted and declined
- **Applications**: The total number of applications received, booked, and declined
- **Rule Performance**: The performance of fraud rules and strategies in production to identify fraudulent activities

Once the key metrics are identified, a sound mechanism to identify sources of fraud losses must be designed. This could include using behavioral charts, a Sigma technique which helps identify outliers based on a predefined multiplier to the standard deviation from historical data. This can be then further sliced at various levels to drill down to the core of the issue. KPIs are tracked for risk categorization, and triggers can be escalated once acceptable levels are breached for different controls that are in place. For example, this could include a sudden increase in the number of applications coming from a particular channel and area.

Mitigation

Once a good understanding of fraud trends and key problem areas are established, the next step is taking the necessary actions to mitigate such trends. Predictive analytics plays a role here to identify and predict segments with high fraud rates so the fraud attack can be intercepted and prevented. Analytics must be blended with deep domain expertise for desirable results. Each type of fraud needs a customized mitigation solution, keeping in context the different themes and actions that happen behind the scenes to purport such fraud.

Account Takeover

ATO fraud typically follows certain steps.

- Fraudsters identify potential targets, such as customers with high credit lines and/or senior citizens
- Fraudster gain access to potential target credentials
determine what’s not natural for a genuine customer, and when the bank should start interdicting suspicious online activity and account changes. This helps banks prevent fraudsters from entering banking systems.

**Transactional level**

If a fraudster gets ahold of a physical card, they typically use it at ATMs, jewelry stores, and other places where they can maximally exploit the card. Such out-of-pattern spending combined with series of account changes, such as a phone number or address change, followed by a request for additional card are used in segmentation to decline probable ATO transactions and subsequently send such cases for manual review.

In case of ATO fraud, since fraudsters has relevant information on accounts to verify and there is a good chance of fraudster passing account verification checks and continuing fraud run, therefore segmentation on verified accounts transactions is performed separately. Combining the customer attributes from their digital journeys with transaction-level data helps analytics build robust ATO strategies.

**Fraud Applications**

Fraudulent applications for credit approval can occur in several ways.

- A fraudster applies for card using personally identifying information (PII) of someone they are well acquainted with, such as a divorced person using their ex-spouse’s PII to get a new credit account.
- A fraudster uses random combination of PII fields to create synthetic ID and apply for new credit account.

This type of fraud can be addressed at two stages:
Acquisition Level

From a bank’s perspective, it’s imperative to filter out fraud application while underwriting real prospective customers. Some of the filtering criteria adopted by banks based on insights from acquisition-level data include:

1. Scrutinizing PII details of incoming applications using a historic list of bad Social Security numbers, phone numbers, addresses, email domains, and other information accumulated over time.
2. Looking for spikes in incoming application from any particular channel or geography.
3. Tagging risky IP address used for pushing fraud applications in the past.
4. Identify links between incoming and existing applications using PII attributes of fraudulent applications and club them in same cluster to identify and mitigate synthetic Id’s and potential credit abuse scenarios.

Transactional Level

Banks can look for unusual spending patterns when developing segmentations to decline probable fraud applications and subsequently sending such cases for manual review. For example, early month on books customer with high utilization rate could be potential cases which can be declined. Similar to the ATO scenario, the fraudster may be able to beat verification. Therefore, segmentation on verified account transactions should be performed and suspicious cases must be reviewed using credit bureau data.

Operations

Operations play a key role in managing alerts created upstream by various fraud identification strategies. It is a bridge between customers and analytics. Fraud mitigation is a two-step process:

1. The first step is identifying and creating fraud strategies driven by analytics and business acumen.
2. The second step involves verifying which channel to use for different strategies, whether through intelligent voice recognition (IVR) systems, text messages, or manual contacts, and their different accuracy levels. Operations plays a key role here.

Several operations components should be designed to effectively balance fraud mitigation and customer experience.

Operations Capacity

There is always tradeoff between alert volume and the operations capacity required to clear the alerts. This can have a large impact on profitability, attrition, and customer experience. Customers want to resume using their card as soon as possible after any possible fraud has been prevented. A few important parameters should be considered when designing this component:

1. How many cases each queue can handle for different channels such as manual contact, IVR and text.
2. The maximum allotted time to clear the account from the queue.

Alert Queues

Every suspicious case cannot be treated equally. Depending on the riskiness associated with a particular fraud case and the type of customer, verification level alert queues should be defined. Generally, ATO cases and accounts which are already verified have very high risks, as the fraudster possesses a certain level of account information and was able to pass the first level of verification. A few things should be kept in mind while creating queues:

1. Riskiness of Alert: Accounts indicating ATO behavior...
should be routed to manual queue, as the level of verification and risk will be higher compared to cases where the fraudster does not possess much information about the account.

2. **Type of Fraud:** In case card counterfeiting, the fraudster does not possess much information about the account. Generally, these cases can be routed to automatic dialers for quick resolutions.

3. **Type of Customer:** Customers who spend more and generate higher profits for the bank would expect speedy resolutions, and should have their alarms routed to the manual queue

4. **Priority Order:** Queues should have priority associated with them. In a scenario if cases can be routed to multiple queues it should be done based on level of riskiness and queue with highest level of verification would take the lead in verification of case

The number of cases worked by manual queues should be minimized due to their high cost. Only certain cases should be routed to manual queues.

- Cases with ATO or fraudulent application concerns
- Accounts already verified

**Authentication**

Given that banks have limited operations capacity there should different levels of authentication in place for preventing fraud. Authentication can be classified by four categories.

1. **Type of Verification:** Verification can be done manually or through automated systems that handle large volumes of requests in a small span of time, reducing impact

2. **Level of Verification:** Cases which have been verified by automated system that must be operated manually

3. **Risk:** High-risk cases like ATO and ID theft must be authenticated manually

4. **Type of Customer:** If the customer is high spender, they will generate more sales for the bank. These should have expedited authentication by proactively flagging and authenticating their card.

Authentication details and questions should be designed in sync with alert queues and inputs from the analytics team. In ATO-related cases, fraudsters have more information about the account and can easily pass authentication checks. In this scenario, the detail level of the questions will be different from a counterfeit scenario.

**Fraud Tagging**

Fraud tagging is important to define the total scope of fraud losses. It can be done in two ways.

1. The customer calls about disputed transactions
2. The bank reaches out about transactions deemed potentially fraudulent.

Generally, different types of fraud have different types behavior associated with them. For instance, ATO
fraud sees non-monetary events happening before the occurrence of fraudulent transactions. For lost or stolen cards, the transaction location might be different from where the cardholder generally uses their card. Therefore, it is important that operations works with the analytics team to design a clear mechanism for distinguishing and tagging different types of fraud at the time of verification. This process will help in crafting better mitigation strategies and better identify loss areas.

**Technology**

Technology plays a vital role in realizing results and turning strategies into actionable events that can identify and mitigate fraud, as well as provide a seamless customer experience. Fraud’s dynamic nature makes it important that the technology infrastructure is flexible enough to handle these changes and incorporate new trends and behaviors.

Fraud’s complexity and constant changes can make this infrastructure quickly obsolete if it is not constantly updated. This can be prevented by incorporating a few parameters when designing the technology infrastructure.

1. **Real-Time Action:** The system should be able to impact the desired population without any lag
2. **Integration:** Multiple data sources should be integrated for implementation in different strategies, including monetary, digital and external data sources
3. **Performance Evaluation:** This should provide the flexibility to measure the lift of adding incremental strategies, such as test versus control measurements.
4. **User-Defined Variables:** User-defined variables enable complex trends to be coded into the systems. This could include referring to multiple months of a customer’s behavior profile while creating features in the system
5. **Action System:** This should have the ability to help users take different action as the situation demands, such as certain cases that might require alerts only rather than blocking

6. **Queue System:** This should have the capability to route the different action to different queues as needed
7. **Strategy Performance:** The capability to generate strategy performance reports for every strategy present in the system, providing insight into which strategies should be deactivated or optimized
8. **User Interface/Syntax:** The syntax and user interface should be easy to use

These parameters help seamlessly turn ideas into actions and help effectively manage fraud risks.

**Decision Making Framework**

Return on investment, or ROI, is an important aspect of any fraud risk mitigation program. Fraud strategies are often driven by their false positive rates (FPR) or hit rates. However, these strategies won’t always produce positive ROI.

Multiple factors should be considered when evaluating the profitability of any strategy. For example, declining low-dollar transaction with a 50% hit rate for fraud might not be a profitable strategy, as operations costs could be higher than the fraud dollars saved.

A few important quantifiable and non-quantifiable factors are important for calculating strategy ROI.

1. **Bad Rate/Hit Rate:** This measures how many fraudsters are captured out of the total population targeted. This helps identify the false FPR. The higher the hit rate, the lower the FPR and impact on customers will be.
2. **Operation Costs:** Operations spending should
include the amount spent treating each case through different mediums and channels

3. **Revenue Loss:** Preventing fraud losses also occasionally impacts customers falsely classified as fraudsters, resulting in revenue loss. The actual future sales loss cannot be quantified through the actions taken.

4. **Customer Experience:** The dollar value of customer experience cannot be calculated, but one study showed that falsely classifying certain customer transaction as fraudulent increases customer attrition.

Combining these metrics helps evaluating strategy performance and balance the factors needed to develop a long-term portfolio strategy.

