Guide

Building a business case for identity verification and risk assessment technology

Introduction

While investment in best-in-class identity verification and risk assessment tools may be substantive from an integration standpoint and because of ongoing transactional costs, the business case for such a project is most compelling when it includes a broad range of elements. Most obvious are those elements associated with fraud loss reduction and prevention at both the account and portfolio levels. Clearly, this is an anchor point, but one to which other elements and factors must be added. The summary below articulates additional line items that should be considered and factored into an overall return on investment analysis when building a business case for a tool to help your organization with identity verification and risk assessment.

Direct measures

Justifying investment in fraud prevention technology can be challenging. From quantifying the impact on the customer experience to estimating the cost of complying with complex regulations, businesses struggle to understand fraud prevention's value and its impact on the bottom line. There are, of course, a number of direct measures that can be more easily quantified with a little research.

Fraud loss detection and prevention

Aite Group recently reported that credit card application fraud losses will grow to $2.1 billion in 2020, while demand deposit account application fraud loses will reach $649 million. In combatting this growing trend, Juniper Research estimates that investment in online fraud detection and prevention solutions will increase 22 percent from 2017 to 2022. We are transitioning from regarding fraud as a "cost of doing business" to fraud mitigation being that cost. Managing and mitigating fraud risk and continuously monitoring performance to adjust your strategies will let you be profitable while ensuring everyone is protected. Consider the following points when making your business case.

- Average loss per account reduction:
  - Predictive decisions detect more fraud attempts prior to loss and minimize the length of fraud events and the window of perpetration. This happens as better-performing models and workflows contextually invoke the right methodologies at the right time.
- Attack rate monitoring and reduction:
  - By understanding current application attack rates and implementing a higher level of deterrence, organized fraud efforts will be pointed to other applications or opportunities in the marketplace.

Current data points to review

- Average fraud loss per application per:
  - Acquisition channel
  - Product
  - Fraud type (identity theft, synthetic identity first-party)
- Average loss per existing account (account takeover)

Operational cost reduction

The fraud landscape is constantly evolving. Schemes continue to rise in sophistication; new and improved prevention technology keeps being developed; and regulations come, go and change. Keeping up with this landscape is complex and challenging, and often causes overlap and duplicated time and effort — which, in turn, increases your operational costs. Here are some common areas where cost avoidance can occur in your fraud prevention strategies.

- Outsort rate optimization — ensure that all applications or transactional (monetary or nonmonetary) requests requiring additional review (versus real-time approval) are fine-tuned to reduce operational costs.

Examples include:

  - False positive rates that don't eclipse fraud loss prevention with the opportunity costs, and any lost revenues associated with "good" applications and actual declined transactions.
  - Costs of outsort review and decisioning that are easily defensible based on a high return on that transactional investment.
  - A target-rich set of reviewable applications or transactions that represent a high and improved level of overall fraud detection within a current or even reduced outsort population percentage of overall volume.
- Elimination of extraneous, ineffective or redundant services.
  - Remove any overlap in multiple services and ensure that performance gaps are closed with best-in-class tools.

Data points to review as you evaluate current solutions include:

- Real-time and near real-time approval rates.
- Outsort rates per channel and per product.
- Fraud detection rate and false positive rate per review queue.
- Cost of application and account review per human resource and aggregate treatment tools/methodologies.
- Cost of lost good customer acquisitions and existing customers.

Strategic cost efficiency

- When justifying the investment in a fraud prevention platform, consider the positive impact the solution can have on business performance.

Value can be found in:

- Better informed and prioritized investments in current and emerging technologies.
- Future-proofed investment in a single integration and platform that allows ongoing expansion of service calls, use cases, emerging technologies, and workflow and decisioning strategies.

Current data points to review and target for improvement:

- One- to three-year road map for identity verification and risk assessment projects and investments.
- Internal validation and testing costs.
- Direct vendor integration costs.
- Operational costs in aggregating multiple disparate service calls for comprehensive decisioning.

Indirect measures

In addition to the areas where you can directly attribute value from the investment in fraud prevention technology, there are indirect benefits. Here are several areas to consider:

Customer experience improvement

Forrester Research reports that the number one priority for 72 percent of businesses is customer experience. With such a strong focus on service and convenience, components important to building your case include:

- Reduced customer impact and exposure to fraud victimization.
- Minimized customer inconvenience.
- Improved customer satisfaction and loyalty through more effective fraud detection and prevention coupled with less unnecessary friction and more positive and passively attained recognition.
- Higher upsell or cross-sell opportunity and fulfillment.

Reputation and brand protection

While the monetary cost of fraud losses can be high, the impact that a loss or breach can have on customer relationships and brand integrity can be even higher. A single incident can destroy the credibility built over the years.

- Reduced exposure to high-volume, high-loss and high-impact fraud events typically associated with new product launches, new customer access channels or applications, or shifts in addressable markets.
- Resilience to the dynamic nature of fraud perpetration driven by high-volume data breaches, a shift toward identity related schemes versus card-present schemes, and more sophisticated fraud attacks.

Compliance

There are many fraud compliance requirements altering the way organizations operate. It has been estimated that noncompliance costs an average of 2.65 times more than investing in a technology-based compliance solution. As you consider the rules and regulations you must meet and how you will meet them, also keep in mind the significant potential costs of noncompliance:

- Penalties
- Legal costs

In this competitive business landscape, you must have cost-effective, flexible tools — solutions that help meet current and future guidelines, operate efficiently, manage risk, and ultimately authenticate as many good customers as possible. Understanding the benefits of such a robust program that supports risk mitigation and the customer experience is essential to building the business case for fraud prevention.

Creating a business case isn't easy — but our experts can help.

Let's get started

Experian
475 Anton Blvd.
Costa Mesa, CA 92626

T: 1 888 727 8330
www.experian.com

09/17 • 2000/1300 • 1147-DA