The First Line of Defense in the Battle Against Fraud

Fraud Detection

Who should read this paper

Consumers' relationship with your company depends entirely on their confidence that you are protecting their information and their privacy. An effective fraud detection system won't complicate users' online experience. Instead, it lets consumers interact with you online without changing their behavior or installing anything on their computer. It makes them feel safe and welcome by learning their behavior, protecting their account information, and responding appropriately to risk with knowledge of internal changes as well as global fraud patterns. This white paper details the criteria that organizations should use when choosing a fraud detection system to protect their organization and their customers.
Fraud Detection
The First Line of Defense in the Battle Against Fraud
A relationship with consumers

By necessity, companies have become deeply trusted confidantes in the anonymous world of the Internet as consumers fill their online accounts with the most personal details. Your database may know more than your consumers’ closest friends and family: bank account balances, retirement savings, credit history, health history, buying habits, entertainment preferences, and more. When consumers create a logon, they enter a relationship with your company based on the confidence that you will protect their information and keep it secure.

Have you done enough to protect their trust?

Fraud detection systems can provide the first line of defense against fraud by preventing unauthorized access to private data and accounts. Like security guards, they watch the action until something unexpected occurs. Then they step in to assess the situation and make a decision about whether or not to allow access. An effective fraud detection system lets consumers interact with you online without changing their behavior or installing something on their computer. At the same time, you have a convenient, non-intrusive way to assess the risk of the transaction and respond accordingly.

The convenience and courtesy of the Internet

Despite the increasing incidence of identity theft and rising costs of online fraud, consumers prefer the speed of transacting online and the convenience of having information at their fingertips, no matter where in the world they choose to log on. A 2011 study by the Ponemon Institute demonstrated that customer turnover in direct response to breaches remains the main driver of data breach costs, and indicated that organizations’ efforts to address the potential sources of data breach are critical to building customer confidence, and lowering the number of present and potential customers who take their business elsewhere. An effective fraud detection system can help companies offer consumers a safe and secure online experience that encourages engagement and creates loyalty to their brand and services.

Invisible protection

The best fraud detection systems are like the most discrete security guards. They have excellent instincts, lots of experience, and a firm, but friendly, approach to resolving disputes. They understand that each user is different while recognizing consistent individual behavior. They also know that attackers continuously evolve their methods and try to adopt the guise of a legitimate user. The following sub-sections provide a short list of qualities to consider when choosing a fraud detection system as the first line of defense for your online applications.

Excellent instincts

Of course machines do not have instincts, but they do have a systematic way to analyze interactions. Most fraud detection systems use a rules engine, a behavioral engine, or both to assess the level of risk. The better the detection system, the more effectively it can prevent fraud without slowing legitimate transactions.

A rules engine reviews a transaction to determine whether or not it has broken a rule before permitting access. A rule might set a maximum number of passwords that a consumer may try, or prevent the creation of a new account with the same email address as an existing account.
The configuration of rules and corresponding interventions have a broad range of effectiveness. A rules engine that is too loose provides spotty protection. A rules engine that is too tight will slow down consumers, causing frustration and increasing support calls. A rules engine that is easy to modify allows a company to adjust the rules to an appropriate risk level to address specific business needs.

A behavioral engine learns how a consumer uses the system to dynamically identify risk. It responds when consumer behavior changes, even if the change does not break a general rule. For example, a behavioral engine goes on alert when a consumer who always logs on from home suddenly logs on from another country. The same behavioral engine does not interfere when a consumer who regularly logs on from different places in the world changes location. A fraud detection system with both rules and behavioral engines does not require a consumer to change behavior. In fact, it creates value from their consistency to help prevent fraud.

When these engines work together, they can assign a more specific level of risk and apply a more appropriate intervention. Does the consumer need to provide additional proof that they are who they say they are? Or should they be locked out of the system and evidence gathered on their attempts?

Lots of experience

Today’s online applications have become deeply integrated into business systems. Yet many fraud detection systems focus narrowly on user name and password. Fraudsters have learned to exploit this lack of integrated protection through cross-channel fraud. They authorize themselves for access by calling support, using interactive voice response systems or chat to change existing account information. An effective fraud detection system takes a broad view of data and activities to respond to the constantly changing tactics of fraudsters.

First, a fraud detection system should broaden its internal scope beyond logons to review data from all relevant systems. For example, an online banking application should apply fraud detection to log on as well as customer telephone support and transaction data to detect anomalies. The IP address of an attacker is an essential source of information for fraud detection. The system should be able to identify the geographic location, connection type, and Internet service provider (ISP) based on IP address. It should then correlate the information with internal data as well as watch lists and global attack patterns. To manage the exponential growth in data without slowing transaction time requires a highly scalable and reliable detection engine.

Second, the more your fraud detection system knows about external activities, the better it can protect consumers and business assets. The objectives of attackers have evolved from high-profile break-ins to achieve notoriety to organized criminal organizations targeting high-value information for profit. An attack method that works on one bank or healthcare system will be shared across the criminal organization and quickly exploited until security systems adapt to shut it down. A fraud detection system that has eyes and ears tracking global trends will be able to recognize new types of fraud and quickly respond with policies to block attacks.

Firm and friendly intervention

Your online applications are much more than a convenience or a way to reduce customer support costs; they create a very personal and private relationship between you and your consumer. Adding a complicated logon sequence that requires users to master your interface or a fraud detection system that constantly disrupts their activities discourages consumers from online activity. A fraud detection system should work in the background and intervene in a firm, but friendly way when appropriate.

A fraud detection system provides an invisible layer of protection between you and your consumer. When risky behavior is detected, an appropriate response will make legitimate consumers feel safer rather than inconvenienced. Risk-based authentication uses the level of risk detected to determine how the system will confirm the identity of the consumer. The system administrator controls whether the system uses
a low-level authentication method such as a security question and response or image recognition, or requires stronger authentication such as an SMS message, an email, an automated call or a customer service call.

In addition to risk, your consumer’s profile may also determine the response. Some fraud detection systems allow consumers to manage their preferred method of notification such as an SMS message, an email, or phone call. You may also decide to apply risk to consumers differently. For example, a moderate risk detected from a high-value or premium consumer may be set to always generate a customer support phone call.

In the case of an attack or breach, the system should help the company resolve the problem quickly while collecting necessary evidence for dispute resolution or potential legal action.

The first line of defense against fraud
An effective fraud detection system makes consumers feel safe and welcome by learning their behavior, protecting their account information, and responding appropriately to risk with knowledge of internal changes as well as global fraud patterns. An effective fraud detection system features:

- Easy-to-use rules engine and a self-learning behavior engine to effectively manage risk.
- The scale and flexibility to combine data from call centers and other relevant systems with transaction and log on monitoring as well as global security intelligence.
- A choice of real-time intervention methods for authentication including challenge/response questions as well as email, SMS text messages, and automated phone calls.

Preventing and protecting against fraud helps businesses deliver convenience and confidence to consumers with comprehensive protection for online applications and transactions.
**About Symantec**

Symantec™ is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com