Entrust® Securing Digital Identities & Information

Fraud Detection Solutions

Top 8 Questions You Should Ask Before You Buy

When it comes to detecting fraudulent activity, a number of solutions are available in the market that can help defend, adapt and protect against cybercrime. But what approach is best? To help sort through the vendor hype, Entrust offers the following list of questions you can ask while evaluating different solutions.

1. Do you have to send your data outside the organization to be analyzed?

2. What is your fraud rate capture?

3. Once new fraud patterns have been discovered, how quickly can the system be updated to start catching these types of fraud?

4. Once you have identified the fraud patterns and implemented the new rules, is your system effective in detecting it 100 percent of the time when it happens?

5. How effective is your fraud system in handling the IVR and call center channels in addition to the online channel? Can it stop fraud across those channels?

6. Does the fraud platform allow you to STOP the fraudulent transactions before the money leaves the financial institution?

7. Does the system allow you to do forensics on transaction histories to find other incidents of a fraud pattern or how a newly discovered type of fraud was perpetrated?

8. Now that you've caught the fraud, how are you going to prosecute?

The Bottom Line: Do you have a zero-touch fraud detection solution with minimal impact to customers and your infrastructures that simultaneously protects your customer institution and your brand?

The following pages will explore why these questions should matter to you and how Entrust's solutions addresses them.

According to Gartner...

- Financial losses due to cybercrime will not peak before 2011, when they will total at least 10 times their current value
- Through 2009, the finanical damage experienced by businesses because of targeted attacks will increase at least five times faster than damaged caused by mass events
- By the end of 2007, three out of four organizations will be infected with financially motivated, targeted malware
- Through 2007, 40 percent of banks and other financial services providers will adopt real-time fraud detection in addition to stronger authentication for online consumer service security

"Predicts 2007: Maturing Information Security Market Must Adapt of Face Contraction," Gartner, November 2006

Fraud Detection Solutions

1. Do you have to send your data outside the organization to be analyzed?

Why does that matter?
If you send your data outside the organization you may lose control of it, risking a potential data breach in the transfer.

How does Entrust help?
An onsite, zero-touch fraud detection solution, Entrust TransactionGuard allows organizations to maintain complete control of all sensitive data at all times.

2. What is your fraud rate capture?

Other considerations…
Do you use open fraud intelligence information to increase your discovery rate? Do you have access to shared information about the use of open proxies, anonymous proxies, host reputation data from other financial institutions and online businesses?

Why does that matter?
Monitoring only specific transactions limits a fraud analyst team's ability to accurately identify normal usage patterns and potentially fraudulent activity. Leveraging a wider range of activity monitoring enables organizations to identify and react to changing fraud patterns in quick, efficient manner. Most fraud detection solutions purposely don't open the aperture of activity for examination because this leads to a higher rate of false positives, which increases the number of staff required to effectively manage suspicious activities and may unnecessarily interfere with user experience. Regardless of what is being monitored, the solution needs to ensure that the ratio of actual fraud incidents is high relative to the total number of flagged activities. This becomes imperative when combined with two-factor authentication, as you don't want to force a large number of legitimate users through unnecessary extra steps, nor needlessly burden your fraud team with a high rate of false positives.

How does Entrust help?
Entrust TransactionGuard monitors all transactions, not just a small, select group. We also offer the Entrust Open Fraud Intelligence Network (OFIN), which provides comprehensive independent fraud data plus known fraud behaviors that have been validated by some of the largest financial institutions in the world. OFIN includes information gathered not only from within the network of global financial institutions, but also supplemental information, such as host reputation data from more than 130,000 submission points that are financial institutions and non-financial institutions. For example, bot-nets typically are used for multiple types of fraud and attacks inside and outside of the financial institution community, and this may be a precursor to an impending attack. The ability to see this behavior can serve as an early warning system in some cases. Finally, Entrust TransactionGuard's ability to see all transactions, combined with OFIN data and a sophisticated rules engine, delivers a more efficient and effective solution for fraud detection.

3. Once new fraud patterns have been discovered, how quickly can the system be updated to start catching these types of fraud?

Other considerations…
If you know about the fraud and cannot update the system fast enough to catch it, will you be able to recover all of the lost funds? What will the increased losses be? What will end-user reactions be?

How long will it take to codify the rules, test them and integrate them? How much development will be required to change your Web application to do call outs for the events you want to monitor?

Does your system require back-end integration with applications? This is much less flexible than a system that serves as a network tap.

Why does that matter?
Network tap-style fraud detection systems are a nimble, flexible approach to transaction monitoring and can be easily updated to detect and defend against new fraud patterns. If you are not using a zero-touch or network-tap approach, it can take a significant amount of time to react to new types of fraud. Solutions that must be integrated with applications for every transaction that needs monitoring will require that each application be changed when new patterns are

More than 100 million Americans have had their personal information, such as social security numbers, medical records and account information compromised since February 2005.

-Privacy Rights Clearinghouse, December 2006

Financial losses stemming from phishing attacks rose to more than $2.8 billion in 2006. In addition, back-end fraud detection and the emerging use of stronger consumer authentication systems seem to be slowing down the rate at which the criminals can raid financial accounts.

- Gartner "Phishing Attacks Leapfrog Despite Attempts to Stop Them," November 1, 2006

discovered. This not only can take months to update but will be a resource-intensive process that will need to be implemented within strict production deployment guidelines, such as no service disruptions within certain periods. This slow reaction time means that fraud will not only continue until the changes are implemented, but it will also continue to evolve and adapt. Not only is there a risk of fraud happening between incident discovery and change completion, but also that you will continually be behind the times in a fight against a highly organized set of criminals.

How does Entrust help?
Entrust TransactionGuard is able to translate and apply new rules in near real time for newly discovered fraud behaviors, all without impacting the application because of its zero-touch nature. This gives the fraud team the ability to make changes themselves rather than relying on the IT department to open applications and update the system to catch new fraud patterns. Updates can happen almost immediately and begin to detect and defend customers without having to wait for the period of regularly scheduled application updates.

4. Once you have identified the fraud patterns and implemented the new rules, is your system effective in detecting it 100 percent of the time when it happens?

Why does that matter?
If your solution isn't monitoring all the transactions or doesn't profile individual user behavior, it cannot adapt quickly to defend against emerging fraud attacks. Without that breadth, it also will not have a high detection rate.

How does Entrust help?
Entrust TransactionGuard monitors all transactions and builds user behavior profiles, which serve as a critical enabler for rapid implementation of new rules to stop freshly discovered types of fraud. Once a fraud pattern has been identified inside of Entrust TransactionGuard and a rule deployed, it will catch that behavior 100 percent of the time.

5. How effective is your fraud system in handling the IVR and call center channels in addition to the online channel? Can it stop fraud across those channels?

Why does that matter?
Fraud attacks are not limited to just one channel. If modification of the application is required, each channel added makes the cost and complexity increase significantly. Also, if you want to do risk-based authentication by leveraging the fraud detection solution, the authentication solution needs to have a range of authentication choices that can transcend multiple channels. Otherwise, you will need to add stove-piped authentication types, which increases cost and infrastructure maintenance needs.

How does Entrust help?
Entrust TransactionGuard is built on open standards and monitors HTTP/HTTPS traffic streams for fraud. New-generation IVR, ATM and other electronic applications all leverage the HTTP protocol for data transmission, enabling Entrust TransactionGuard to easily monitor the Web as well as add other channels into the fraud detection equation. To enable risk-based authentication, Entrust TransactionGuard integrates seamlessly with Entrust IdentityGuard, a versatile authentication platform with a range of authenticators that can be used to more strongly authenticate users not only online, but also across other channels.

6. Does the fraud platform allow you to STOP the fraudulent transactions before the money leaves the financial institution?

Why does that matter?
Solutions that don't monitor all transactions are limited in their ability to stop all fraud — even if discovered — as they cannot react quickly to new patterns. In addition, fragmented solutions that do not integrate fraud and authentication capabilities out-of-the-box require the deployment of multiple services and/or software components to offer different types of authentication. Being able to integrate the risk assessment done by the fraud detection solution in real time with the authentication platform makes it possible to use stronger authentication, or even block access when the risk associated with a user logon or transaction is too high. The fraud is avoided rather than merely detected after that fact, but only if the two solutions can be easily used together as appropriate.

How does Entrust help?
The Entrust Risk Based Authentication Solution, which combines Entrust TransactionGuard and Entrust IdentityGuard, enables real-time risk analysis for online transactions with the ability to interdict and strengthen authentication, or even block access when the risk associated with a user logon or transaction is too high. A versatile authentication platform that provides a range of authentication methods, Entrust IdentityGuard seamlessly integrates with Entrust TransactionGuard, allowing maximum choice for risk-based authentication — all from a single platform.

7. Does the system allow you to do forensics on transaction histories to find other incidents of a fraud pattern or how a newly discovered type of fraud was perpetrated?


Why does that matter?
With a system that just sends the data offsite for analysis, you will be unable to identify other instances of the new fraud pattern. Even if you can get access to the data that was sent offsite to the vendor, solutions that only capture select transactions will not have the ability to track behavior across channels or piece together patterns of behaviors across transaction types that are not monitored. This makes it incredibly difficult to piece together the entire picture of how a fraud was perpetrated, and you likely will miss earlier indicators that would serve as a red flag for impending fraudulent activity if you had a system that capture all the data across all channels.

How does Entrust help?
Entrust TransactionGuard captures all relevant data for fraud analysis on current and past transactions, and the organization stores the data on their premises, making it available for retrieval and analysis at all times. This enables the ability to see other instances of the pattern historically, allowing organizations to identify other occurrences of crime that may have happened before the fraud pattern was discovered. Organizations that take a proactive approach to identifying and making restitution with customers before the customer discovers the fraudulent activity stand to gain higher customer loyalty than ones that wait for the customer to find out they have been a victim on their own.

8. Now that you've caught the fraud, how are you going to prosecute?

Other considerations…
If you decide to turn off the service, can you take any of the data or fraud rules with you? Do you own them or does your vendor?

Why does that matter?
With a system that just sends the data offsite for analysis, you will be unable to create the necessary paper trail to give you enough evidence to prosecute the criminals once the fraudulent activity is identified. Even if you can get access to the data that was sent offsite to the vendor, solutions that only capture select transactions will not have the ability to track behavior across channels or piece together patterns of behaviors across transaction types that are not monitored. Any evidence you could collect in hindsight will be incomplete. In addition, some service-based solutions are simply gone when they are turned off — all data and rules are lost. Make sure you find out if you own the fraud data and rules once you decide to turn the service off. In addition, ensure that the vendor delivers an approach to capturing fraud behaviors that is standards-based so that the knowledge gained during a deployment is transportable.

How does Entrust help?
Entrust TransactionGuard captures all relevant data for fraud analysis on current and past transactions, and the organization stores the data on their premises, making it available for retrieval and analysis at all times. This helps not only for collecting evidence to prosecute criminals, it also enables organizations to control all aspects of their fraud detection system, including both data and fraud rules/behaviors that have been implemented. In addition, Entrust TransactionGuard and the Entrust Open Fraud Intelligence Network support a draft standard currently in the IETF focused on standardizing fraud behavior sharing, removing risk around the loss of critical knowledge on fraud. If an ongoing service agreement is discontinued, you own all of the rules and behaviors that have been collected to date. You only lose the ability to detect and defend yourself against any new patterns that may arise after service is discontinued, but at least you won't become a victim of the old patterns that had been effectively thwarted.

The Bottom Line: Do you have a zero-touch fraud detection solution with minimal impact to customers and your infrastructures that simultaneously protects your customer institution and your brand?

About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,650 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

Entrust® Securing Digital Identities & Information