Entrust® Securing Digital Identities & Information

Fighting Fraud in Today's Connected World

Critical approaches to affordable fraud detection

July 2009

Table of Contents

1 Introduction

Perpetrating fraud for financial gain is not a new phenomenon; it has been around for centuries. Likewise, protecting innocent consumers from fraud schemes is not a new concept. Law enforcement agencies continually strive to keep pace with innovations in fraud by investing in intelligence-gathering and investigative techniques to catch and prosecute offenders while using the knowledge gained to help prevent future occurrences.

During the past 20 years, financial transactions have increasingly evolved from paper- and hard currency-based methods to electronic-based systems, with credit cards and inter-bank electronic transactions leading the way. The move to electronic commerce methods has not deterred criminals. In fact, this advancement has created new opportunities for them to globally exploit consumers and institutions by using increasingly sophisticated fraud techniques not possible in the physical world.

In response, computer-based fraud detection platforms have been introduced to help identify illegitimate credit card transactions and money-laundering schemes.

Traditionally, fraud detection platforms have been integrated directly into banking applications and have used a statistical analysis-based approach for detecting fraud. While a best practice at the time, these fraud detection platforms took months to deploy and implementing any changes to the banking application or the fraud model involved significant time and effort.

Today, financial institutions are offering more and more online and self-service applications, as well as expanding the methods that consumers can use to access these applications. From Internet-based banking to telephone, ATM and now mobile-based access, banks are continually expanding their offerings to meet consumer needs and help increase their bottom lines.

With the constant addition of new banking applications and access methods, financial institutions are now faced with the challenge of having to keep pace with the criminal threats targeted at their business. Translating data found from traditional methods of fraud detection is proving to be too expensive, time-consuming and slow to react to the fast-paced world we live in today. As such, new approaches to real-time fraud detection have emerged, promising to address the shortcomings of traditional approaches.

Unfortunately, while several of these new methods bring new capabilities — frequently when deployed in isolation — they often fail to provide the comprehensive protection against today's criminal threats. Ideally, the most effective fraud detection approaches will integrate a number of approaches — leveraging the strengths of each — to provide the best line of defense against fraud threats.

This paper discusses the evolving fraud world; from the incredible growth in the sophistication of criminal attacks to the various approaches that can be used to help monitor and prevent fraud threats from succeeding. It introduces Entrust TransactionGuard, a zero-touch fraud detection platform that employs a layered approach to fraud detection, providing financial services organizations a reliable defense against today's real-world criminal attacks and the ability to evolve to help address newer threats.

2 Trends in Online Banking

Rapid Growth of Access Methods and Service Offerings

Online banking has taken off — in volume and in scope. There is a migration away from in-branch banking that has been beneficial for both consumers and banking institutions. From Web-based banking to telephone-based IVR banking, from mobile banking to online ATM kiosks, consumers have embraced and come to depend on this self-service model.

Along with offering customers these new access methods, banks continue to migrate more and more of their existing services to the online channel, introducing new applications often in order to reduce costs and increase consumer satisfaction.

Rapid Growth in Attacks

While this migration away from in-branch banking is an appealing alternative for both consumers and banking institutions, it has also provided new opportunities for criminals. The rapid evolution of online commerce systems has been matched by the criminals' abilities to exploit these systems — and from anywhere in the world. Research from organizations such as Gartner and the Anti-Phishing Working Group highlight mounting evidence that online fraud is expanding at an alarming rate.

Driven by the opportunity to make vast sums of money through defrauding financial institutions, criminals are rapidly improving their fraud abilities with significant investments in advanced technology, resources and people. They are becoming increasingly sophisticated in their organization and attack methods. A reflection of the large opportunity, fraudsters now use well defined business processes, role specialization, supply chains and tool-sharing, enabling them to quickly adapt to organizations' attempts to secure their commercial sites.

Online criminals have developed and continually enhanced their fraud methods, which they exchange openly within the criminal underworld in order to increase profits. Without the proper tools, organizational structure and network of allies, financial institutions simply cannot keep pace and stand to lose significant ground with potentially devastating consequences.

Fraud on the Rise

- The number of phishing sites peaked at over 27,000 in 2008[1], with the highest point of turmoil in the financial services industry coinciding with the peak of attacks
- More than 5 million U.S. consumers lost money to phishing attacks in the 12 months ending in September 2008, a 39.8% increase over the number of victims a year earlier [2]
- Crime-ware malicious code hit an all time high of over 1500 unique applications in 2008 [1]
- In the UK alone, online banking fraud losses experienced a 132% increase from 2007 losses [3]

[1] "Phishing Trends Activity Report," Anti-Phishing Working Group, March 2009.

[2] "The War on Phishing Is Far From Over," Avivah Litan, April 2, 2009, Gartner, Inc.

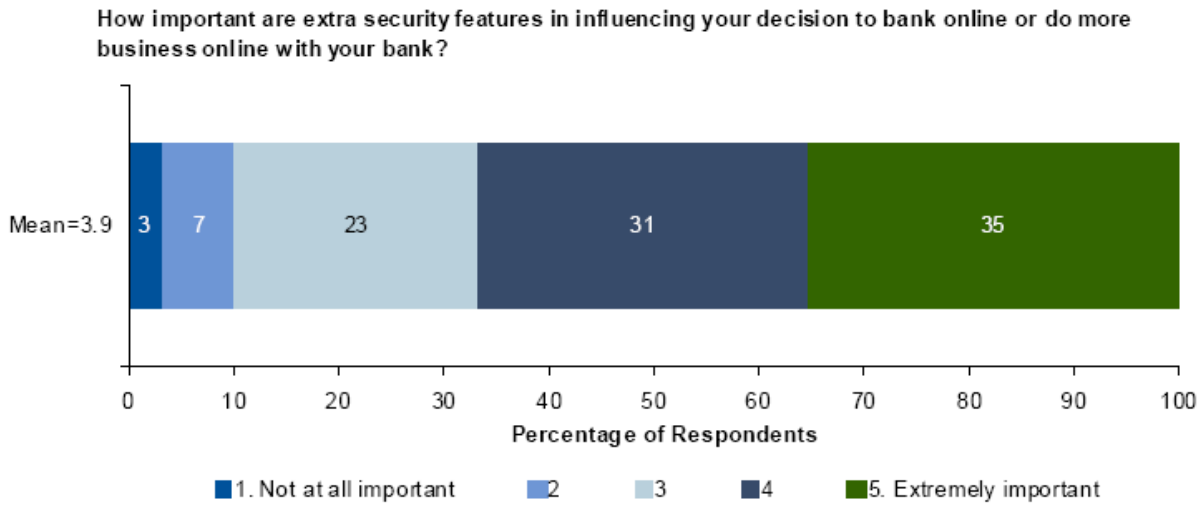
[3] "APACS," UK Payments Association, March 2009.

Erosion of Consumer Confidence Placing Online-Banking Growth at Risk

Banks are interested in minimizing losses from online identity theft; however, the loss of consumer confidence in the banks' ability to protect their funds is of far greater concern. Studies show that consumer confidence is critical to sustaining the online-banking trend. As more consumer breaches occur, there is an increased likelihood of a decrease in online-banking usage — or worse yet, a loss of customers to the competition.

The risk of having to weather such consequences is driving banks to deploy fraud detection solutions designed to address the threats and fast-paced changes in today's connected world.

Figure 1: Putting Security Into Perspective



Source: Gartner (February 2009)

Mounting Pressure from Government and Industry Bodies

New industry regulations around the globe are pointing to the need for real-time fraud detection solutions to address today's advanced online fraud techniques. Organizations must not only meet requirements spelled out in regulations that specifically apply to them, but must evaluate and learn from the guidance in other regulations to enable them to develop best practices in the fight against fraud. Global regulations each contain important fraud prevention techniques and best practices such as:

- The United States banking community's FFIEC guidance highlights the need for increased online user protection, leveraging authentication and real-time fraud detection.
- The U.S.'s pending FACTA Red Flag guidelines outline the need to monitor a variety of red flags of fraud, including patterns, practices and activities.
- The United Kingdom's Faster Payments Initiative (FPI) will speed the processing of financial transactions to clear in seconds versus days, making the need to see potential fraud in real time critically important.

[1] Graph source: "2008 Data Breaches and Financial Crimes Scare Consumers Away," Avivah Litan, Gartner, Inc., February 29, 2009

- The European Union's Payment Services Directive provides the legal and technical framework for all electronic payments in the EU and transfers responsibility for the prevention of fraud to the payment services providers.

Real-time fraud detection consists of two critical elements that squarely address today's online threats:

1. The ability to learn about the latest trends in fraud, either internally through sophisticated data analysis or through external sources
2. Using up-to-date fraud information, organizations can rapidly respond to new types of fraud and makes changes to their systems to help prevent the latest fraud techniques and variations

Real-time fraud detection also requires the ability to quickly react and to understand what to look for using the latest fraud information. The challenge is that most organizations have not found effective ways to rapidly translate learned information into making live fraud detection more effective.

3 Critical Considerations for Fraud Detection Deployment

From a wide range of tools to a variety of solution approaches, financial institutions are faced with numerous options and alternatives for addressing online fraud, which can be difficult to assess and often seem mutually exclusive of one another. Evaluating how to move forward with implementing a solution can seem like a risky proposition in itself, although the costs associated with not taking action are even more daunting.

While there are a myriad of factors to take into account, the critical considerations when evaluating a fraud detection solution are cost of ownership, effectiveness, impact to the user experience and differing detection strategies.

Cost of Ownership

While assessing a vendor's product licensing costs is fairly straightforward, understanding the underlying implementation and ongoing maintenance and operations costs can be more challenging. Will changes be required to back-end banking applications? How often are the banking applications and the fraud system changed to accommodate new needs? Will new applications be coming online that require fraud detection?

Financial institutions typically have a number of online-banking applications to meet the diverse needs of its banking clients and continually developing new applications to support new online services. When evaluating an investment in a fraud detection solution, it is critical that integration effort, as well as upfront and ongoing costs, associated with making changes to the back-end banking application are assessed.

Some fraud detection solutions require direct integration to each of the banking applications being protected, forcing the need for extensive modifications every time a banking application is changed, a new application is introduced or a new fraud pattern is encountered. This results in a high total cost of ownership and a highly risky proposition for the bank — both in terms of the speed at which fraud is changing today and the gap in implementation direct integration will logically require.
Other fraud detection solutions take a passive integration approach in which the fraud detection solution functions in parallel to the online applications being protected. This non-intrusive

approach means that banks can quickly deploy new fraud rules or start monitoring new applications without the cost and effort of having to modify the back-end banking application.

Solution Effectiveness

There are many factors to consider when assessing the effectiveness of a fraud detection solution. With the number of transactions soaring and fraud attacks becoming more and more sophisticated, a number of metrics must be evaluated.

For instance, is the solution monitoring and catching all instances of fraud? Is it able to quickly adapt to new and emerging fraud threats and make use of new fraud intelligence data? Does the solution enable fraud analysts to understand why alerts are generated and conduct root cause analysis? Are false positives kept to a minimum so that time and money are not wasted? An effective fraud detection solution must include these capabilities and more to enable an organization to effectively identify, trend and combat fraud.

User Experience

The cost of acquiring new customers is no different in the banking world than any other industry — one of the key goals is to ensure customer retention is high, and a customer's experience with your online-banking system will dramatically affect their willingness to stay.

Customers are not only concerned about security, they want the freedom and flexibility to bank according to their needs. If the banking solution continually introduces barriers and delays to their online-banking experience, even in the name of "security," customers will quickly look for alternatives. An effective fraud detection solution enables transparent fraud-monitoring and will only invoke increased security measures when risk warrants it.

Deployment Strategies

Several approaches can be used to help fight online fraud. While many organizations have the ability to analyze logs after transactions have completed, the speed at which transactions are happening today makes this approach less than ideal; real-time fraud detection is required.

While some vendors leverage the traditional fraud detection approach of integrating directly with a banking application, others venture into new architectures that allow for more simplified or rapid deployment and can have a direct impact on the effectiveness of fraud capture rates.

Similarly, a shift is occurring in how transaction data is analyzed. While statistical models have historically proven to be quite effective for billions of credit card transactions, new rules-based models offer the promise of quick response to new types of fraud attacks in the online world.

While banks have always had the option to lock down accounts or credit cards when fraud is suspected, they are seeking new methods that will help to defend against potential fraud without unnecessarily inconveniencing customers (e.g., arbitrarily deploying strong authentication to all users for all types of transactions).

To further explain their importance, the following sections discuss various approaches to solution deployment, transaction analysis and defending against threats in the fraud detection world.

4 Deployment Approaches to Real-time Fraud Detection

Direct Integration with Online-Banking Applications

The traditional approach to deploying fraud detection in an online-banking environment is by directly integrating the fraud detection software with the back-end banking application(s). This relies on custom integration work performed by highly skilled application developers from both the fraud detection vendor and the banking application software designers.

This approach is complex and requires initial and ongoing changes to the banking application. Leveraging this specific fraud-monitoring strategy often only looks at certain steps in the transaction process — typically those steps that involve the most risk if fraud occurs (e.g., when funds are transferred to an external account). Once integrated, the fraud system works as an efficient extension of the banking application.

Where this Approach Works Well
Integrating fraud detection directly into a banking application can be an appropriate deployment approach in circumstances when there are relatively few applications to be monitored and the expectation is that there will be infrequent changes to the banking application or fraud detection system moving forward.

Since the fraud system runs within the bank application, there is very little new hardware — outside of the fraud management system itself — to be purchased and little involvement from the networking side of the IT department. Without additional servers and components to manage, ongoing IT management of the system is usually straightforward.

Challenges with this Approach
While fraud can be monitored effectively using a direct application integration, it is not an ideal approach in environments of constant change (e.g., Web channel). With direct application integration, the initial deployment can be very time-consuming and expensive, as the application must be changed in a many spots in order to effectively monitor the users.

Ongoing, each time a financial institution wants to introduce an enhancement to their banking application or roll out entirely new online services, experts from the fraud vendor must be brought in to work with in-house banking application designers to implement the integration between the two systems.

This can prove to be very costly and add significant delays when trying to introduce new applications. Similarly, when new fraud attack patterns emerge, changes to the fraud system will be required. Since the fraud detection software is integrated to the banking application, both teams of software experts will have to collaborate to ensure the required changes do not hinder the banking application.

The high cost associated with this direct integration approach often leads to decisions being made that focus on cost instead of effectiveness, resulting in only partial deployment of the overall solution. This means only a subset of the banking application is monitored, resulting in gaps in the fraud detection process — gaps that can be exploited by criminals.

"Zero Touch" Integration

With the explosive growth of distributed computing networks, leading modern fraud detection vendors have taken a new approach to monitoring banking applications based on a passive integration approach.

In this model, the fraud detection system "taps" into the computer network and passively monitors the entire transaction stream between the user and the banking system, looking for possible indications of fraud — all without any impact on back-end systems. This "zero-touch" approach is combined with sophisticated analytics and case management that provide organizations with a complete fraud detection solution.

Where this Approach Works Well

Unlike the direct integration approach, there is no need to touch banking applications in order to detect and defend against fraud. Therefore, in banking environments where applications are constantly evolving and new channels (e.g., mobile, ATM, telephone) need to be monitored in addition to online, a passive, zero-touch integration enables a bank to move un-hindered by complex integration issues.

Up-front deployments of fraud detection involve less cost and time when compared to directly integrating with the banking application. Using this approach, minimal effort is dedicated to fitting into the network and ensuring the server platforms are appropriately sized to host the fraud system. Instead, the majority of effort is focused on understanding applications and users while formulating a strategy for effective fraud management.

Within the zero-touch model, each time the bank changes their online application or rolls out additional applications, business analysts can quickly and easily reconfigure the fraud detection solution to start recording and analyzing the new application environments. The cost and speed of rolling out new banking applications, or new fraud detection rules, is minimized and implemented by business or fraud analysts, typically through a graphical-based fraud management tool.

This is much easier to accomplish compared to software developers making programming changes in the back-end banking application, especially when one considers the challenge of change cycles inside a complex environment.

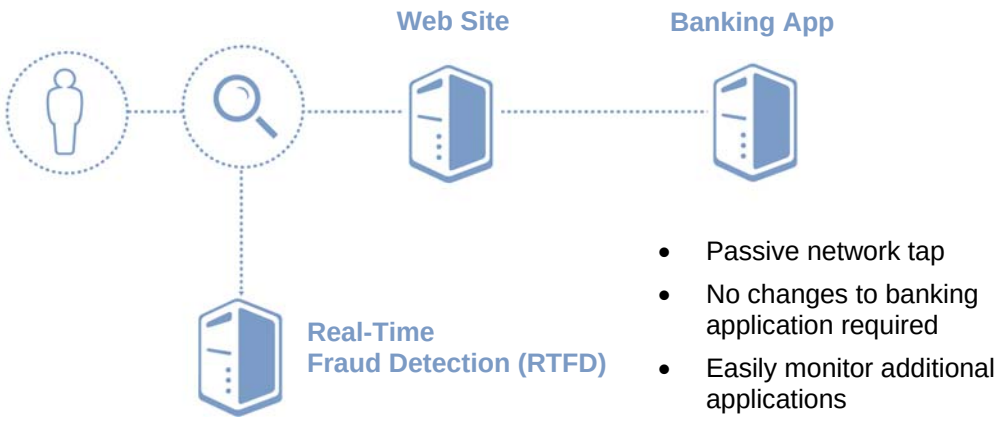


Figure 2: Entrust's Zero-Touch Deployment Model

Unlike direct integration approaches that will normally only monitor isolated points in the transaction, a zero-touch system can easily capture and monitor all transaction activity. While at first glance this may seem unimportant, it is a critical element in transaction monitoring. Often, fraud attacks start out with seemly innocent activity on a users account — maybe simply logging in and checking an account balance or changing an e-mail address.

While typically this is considered "normal" behavior, certain patterns may, indeed, be a clue that a fraud attempt is in progress. For example, if a single IP address is found to be viewing the account balances on 30 different accounts within a short time span, this may indicate a fraudster who recently purchased compromised credentials and is checking to see how many funds are in these accounts.

Challenges with this Approach
Because a zero-touch integration approach is not integrated directly to the banking application, it does require some additional hardware and networking resources to support the deployment.

However, these solutions typically will be implemented on industry-standard platforms that are commonly deployed and supported in most organizations today. In addition, the required changes to the networking architecture are well understood. This means that the deployment steps can be easily supported by routine IT practices and ongoing systems management can be integrated into organizations' existing IT processes with little to no impact.

5 Transaction Analysis Approaches in Fraud Detection

Pure Statistical Data Analysis

Traditional fraud detection solutions are based on pure statistical analysis, typically using either Bayesian or neural network approaches. These approaches use a set of mathematical equations to assess user behavior and generate alerts based on statistically relevant deviations for the "normalized" behavior.

Where this Approach Works Well
Historically, the statistical approach has proven effective for credit card transactions, as the volume of data is huge and the transaction-clearing time can be up to several days, providing time to complete the analysis and deal with any anomalies.

Credit card transactions also have a very simple, inflexible format: date, time, card number, merchant, merchant type and location. Location and merchant type are key elements of modeling user behavior. For example, if a user rarely travels and has very specific spending habits, it is likely that a series of out-of-state purchases of unusual types of merchandise may be fraud.

A pure statistical approach can be effective for monitoring online banking as well. By design, they automatically assess and determine possible fraud instances without a user having to program and manage organization specific rules. This can be very beneficial in situations where a broad number of rules would need to be developed to take into account individual user behavior patterns.

Challenges with this Approach
While providing some value when deployed to evaluate banking, brokerage and credit application transactions for Web sites, a pure statistical model can be less than ideal as a singular solution. This is due to several factors that make the online environment different from the traditional credit card transaction business:

Lower Volume of Data — The volume of these transactions for online access is often much lower than credit card volumes. For instance, trying to normalize transactions and user behavior between Web sites can be problematic because of the low volume of transactions that are not identical. This means that the time required for a neural network to learn to accurately predict fraud is much longer, translating into high false positives.

Huge Diversity of Transactions — Unlike the set format of a credit card transaction, the types of transactions in the online environment are much more varied. They include not just actual financial transactions, but all activities the user engages in while navigating the application. Within a session or spanning multiple sessions and time, the number of possible sequences of user actions is enormous.

In addition, transaction attributes, such as location and merchant type, are much less accurate or don't exist at all in online transactions. This means that more transaction patterns and risk factors must be considered to accurately predict fraud. For example, determining user location based on the geolocation of an IP address can be inaccurate, as IP addresses can be masked or faked. As a result, identifying a potentially relevant deviation is significantly reduced when the statistical model is unable to establish meaningful patterns to start with.

High Rate of Change — Online environments are often subject to frequent changes that affect the types of transactions and their attributes. This negatively impacts the accuracy of a pure statistical approach as the performance is dependent upon the completeness of its "model." As an example, if the model does not include "view e-mail address" because it was omitted from the model or it was modified during a Web site update, the statistical approach will not be able to identify fraud scenarios that make use of e-mail addresses lookups.

Need for Real-Time Detection — Online fraud happens quickly, often in near real time and is getting faster every day. Given this new reality, there is an industry push to evaluate risk and use stronger authentication to prevent fraudulent transactions rather than detecting them after the fact. This means that post-transaction batch processing isn't practical. In a real-time deployment scenario, Bayesian and neural network approaches have a tendency to generate a significant level of false positives when first deployed and for a period of time after initial deployment, thus reducing its ability to detect fraud as it happens.

In addition, it is common practice for some of these solutions to "back-color" transactions, often days later, where the system has seen enough anomalies over a period of time to detect that a given transaction is fraudulent, even though it was initially rated as normal. In a real-time scenario, the transaction my have already been cleared by the time it was identified as fraudulent, further reducing the effectiveness of the statistical approaches in real-time fraud detection.

Understanding Detected Fraud — When investigating suspicious activity detected by the system, it is important to understand why that activity was identified as suspect. An effective fraud detection solution provides detailed information about what lead to the triggered alert, including the specific conditions, transaction data attribute values and user transaction history associated to the incident. In statistical approaches, the reasons that lead to the alert are often much more vague and difficult to investigate.

In summary, while Bayesian and neural network approaches can be effective, used in isolation they suffer from a number of shortcomings that will ultimately have a negative impact on the overall effectiveness of the fraud detection solution.

Rules-Based Data Analysis

Similar to statistical approaches, rules-based systems have been widely deployed for many years. A common example of a rules-based system is in the area of password-based authentication — if the password matches, the rule condition is met; if not, the rule is breached and access is denied.

The main difference is that unlike statistical approaches that identify deviations from what is calculated to be normal behavior, rules-based systems identify what set of conditions constitute fraudulent behavior. These conditions are defined fraud patterns that are customizable to the particulars of a given organization's online environment.

The binary nature of rules means that they can be modified and implemented quickly to identify fraud, while still providing flexibility in detection based on the ability to accommodate partial matching of conditions.

While a rules-based approach is well suited to the dynamic nature of online banking, it also suffers from some factors that the statistical approach takes for granted (e.g., automatic system learning is not inherent to a pure rules-based model).

Third-Party Perspective

"Most advanced fraud managers are asking their vendors that supply fraud scoring technology to provide business users the ability to add their own rules on top of mathematically derived scores.

This way, for example, enterprises can quickly respond to new types of attacks they are subjected to that may not yet be known by the fraud detection model."

Avivah Litan
Vice President
Gartner, Inc.

"Magic Quadrant for
Web Fraud Detection"
February 6, 2009

Where this Approach Works Well

Rules-based approaches don't require a "learning" period, as either a given condition exists or it does not. As a result, rules-based approaches will immediately start identifying suspicious conditions 100 percent of the time — so long as a rule exists defining the suspicious pattern. Rules can also be used in combination with one another, making them effective in reducing the amount of alerts and false positives generated.

For example, the rule: *"If a user attempts to transfer $20,000, raise an alert"* will generate many alerts, including ones for legitimate users conducting such transactions, thus reducing the effectiveness of the system.

However, if a set of conditions are combined to more closely reflect the possible fraudulent behaviors, such as: *"If a user attempts to transfer $20,000 AND the account the money is being transferred to is outside our financial organization AND the user is on a computer that has never been used to access the online banking system OR the user appears to be logging in from Russia, then generate an alert"*, the rules-based solution becomes more effective.

Unlike a statistical-based analysis approach, a rules-based approach can work immediately in a new environment, or in one where low volumes of transactions exist, since no learning is required whatsoever. This means that financial institutions can quickly deploy rules to catch new types of fraud with immediate results. In addition, a rules-based approach works well in real-time fraud detection environments, thereby enabling immediate action such as step-up authentication to be invoked.

Challenges with this Approach

While rules-based approaches can be very powerful, simple to maintain and allow a fraud analyst to easily identify what leads to an alert, they are, by nature, a binary system; they do not take individual user behavior patterns or system-wide activity patterns into account.

For example, while it may be abnormal for User A (with an average transfer of $25 per transaction) to transfer $5,000 to an external account, it may be very normal for User B (who transfer $5,000 every second month to an overseas account) to conduct the same transaction.

While it may be normal for a user to make a transfer of $5,000 to an external account, if 20 users all transfer $5,000 to the same external account within a 30-minute timeframe, this may be an indication of suspicious behavior.

Since pure rules-based systems do not support learning by nature, it can be a significant burden for the fraud department to create new or updated rules as new fraud threats emerge. To address this issue, leading fraud detection vendors should provide customers with a library of continually updated fraud rules templates that can be easily downloaded and personalized by an organization's fraud department.

This, in addition to supporting a simple-to-use fraud rule creation engine, will help keep rule management under control. But ideally, pure rules-based systems could benefit from statistical analysis of transaction data to help incorporate learning into the rules algorithms.

A Blended Approach of Both Statistical & Rules Data Analysis

An ideal data analysis strategy includes a blend of both statistical and rules analysis, taking the strengths of each model to optimize fraud detection effectiveness. Among the market leaders in the Web fraud detection marketplace, the Entrust TransactionGuard platform provides an ideal blend of statistical learning and rules-based analysis, profiling both individual user and system-wide transactions.

The system automatically builds user profiles and monitors patterns, allowing for learning and automatic intervention (i.e., no human involvement) within the system. This strategy of combining rules and a mathematical approach to derive a risk score at any given time is a fundamental capability of the solution that allows for effective fraud capture — providing a more realistic and pragmatic approach — in the fast-paced online fraud world.

6 Defensive Approaches to Fraud Detection

What Activity Is Being Monitored?

Today's fraud attacks are sophisticated and criminals are continually evolving to find new ways to circumvent online security measures. Since the inception of online-banking applications, security has been based on simple username/account ID and password methods. Due to increasing attacks and legislation, many institutions have augmented security with additional methods such as personal questions and image replay.

However, in isolation these approaches don't provide the necessary security for online banking to be secure, driving fraud detection vendors to introduce more reliable methods to defend against online attacks, including:

1. Improving fraud detection at initial sign-on with device profiling
2. Introducing "in-session" transaction analysis
3. Building user profiles to better determine abnormal behavior for each individual customer

Device Profiling

This fraud detection technique analyzes the device (often a computer), as well as network attributes associated with a user when they access a banking Web site. Device profiling can be very powerful, as it quickly determines information such as: Is this a device we have validated in the past (i.e., device tagging, fingerprinting)? Is this a typical access location for this user (i.e., IP-geolocation)? Is the logon pattern suspicious (i.e., groundspeed analysis)?

All of these questions can be very quickly evaluated with device profiling and are totally transparent to the end-user. However, device profiling is not a fool-proof technology. In some cases, device-tagging information can be stolen by criminals; or, users will often make changes to their computer settings such as deleting cookies or modifying attributes that make the computer no longer recognizable as a known device to the banking application.

These challenges simply highlight the need to make device profiling a part of an overall fraud detection strategy; deployed as a complete solution it will leave organizations with large opportunities for criminals to subvert and bypass the system.

In-Sessions Transaction Analysis

Other vendors have opted for an in-session transaction analysis fraud detection, which evaluates the activity a user is conducting in real time, such as changing an e-mail address, paying bills or a transfer of funds to an external account.

In-session transaction analysis can be very effective, as it can be used to track suspicious transaction patterns typically used by criminals, such as changing a mailing address and then ordering checks. It also can look at patterns across multiple sessions, such as 20 different users all transferring $10,000 to the same external account within a specific 20-minute period.

Transaction analysis is also effective in dealing with transactions of high consequence, such as flagging a transfer of more than $50,000 as one that requires further scrutiny to ensure the user is authentic.

Used in isolation, however, transaction analysis assumes the user is valid simply by the fact that they have gained access to the system. Transactions executed by a criminal that "fly under the radar" and appear to be normal can easily circumvent the scrutiny of in-session analysis. As well, without taking into account individual user differences, this method can generate a number of false positives since the definition of what is "normal" is applied across all users in the system.

Third-Party Perspective

"More advanced fraud detection vendors look at user activities beyond logins, such as navigations and transactions. Just examining a login or access to a Web site is not enough for companies that are subject to sophisticated fraud attacks because theses functions are increasingly easy for fraudsters to spoof."

Avivah Litan
Vice President
Gartner, Inc.

"Magic Quadrant for
Web Fraud Detection"
February 6, 2009

Behavior Profiling

The third approach, behavior profiling, builds on the capabilities of in-session transaction analysis by taking into account each individual user as well as groups of users. It automatically tracks user behavior to build up a user profile that may be leveraged for statistical analysis and decision-making.

The profile can then be layered to work with transaction analysis and device profiling to increase the effectiveness in both pinpointing potential fraud while minimizing false positives at the same time.

Authentication Based on Risk

Fraud detection exists for one key reason: to assess, as accurately as possible, if the user accessing the system is authentic. In an ideal world, criminals are stopped before entering the online application while valid users are granted access with ease, allowing them to freely conduct online banking without interruption.

Unfortunately, with the myriad of variables present, it is virtually impossible to consistently accomplish this. Criminals either will gain access by exploiting weak authentication or customers will be burdened with such rigorous authentication schemes that they will abandon online banking all together. How is the defense balanced with user experience?

Rudimentary fraud detection is limited to simply reporting on fraud attacks by generating alerts when suspicious activity arises. These alerts flag fraud analysts that something may be wrong, but analysts have little chance of reacting in real time and the transaction will likely be completed before any action is taken.

Other solutions may have the ability to block a transaction in real time, which may be effective in stopping fraud, but if that transaction is being executed by a valid user with a slightly elevated risk score, they will certainly be frustrated if they are denied access.

Leading fraud detection solutions incorporate risk-based authentication as a key component of their defense strategy so that the system will automatically attempt to mitigate elevated risk without any fraud analyst intervention. The most effective solutions support a broad range of authenticators so that organizations can deploy authentication based on individual user or group profiles.

For example, typical banking customers may be best served with transparent device authentication with picture replay, leveraging a knowledge-based technique for step-up authentication. High-net-worth and corporate clients may be best served by a one-time passcode token or a digital certificate on a crypto token. Mobile users may be served in a variety of ways, including an out-of-band soft token solution.

Similarly, a true versatile authentication platform can support dynamic step-up authentication based on the situation. For example, a user who is about to complete a high-value transaction may be sent a one-time passcode out of band (e.g., e-mail or SMS) to help disrupt a possible man-in-the-middle threat.

7 The Entrust Approach: Trusted Security for Less

Entrust supports the use of fraud detection, strong authentication and extended validation (EV) certificates to help defend against and detect online fraud. This solution is composed of zero touch, real-time fraud detection provided by Entrust TransactionGuard, the Entrust Open Fraud Intelligence Network (OFIN), the Entrust IdentityGuard versatile authentication platform and Entrust EV certificates.

Together, these products provide financial organizations with the means to continually deploy and enhance secure Internet, mobile and ATM banking solutions so that their consumers are protected from online fraud.

Zero-Touch Fraud Detection: Entrust TransactionGuard

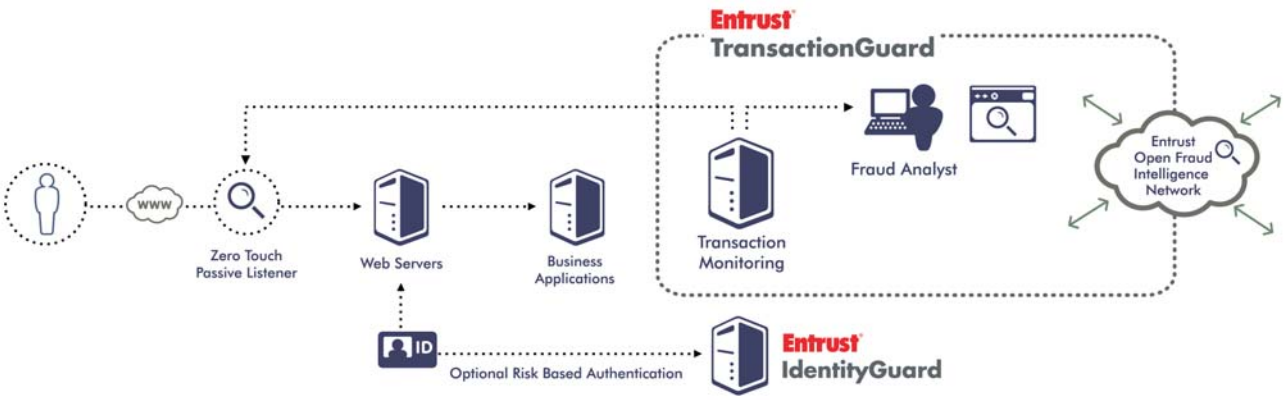
Entrust TransactionGuard can help protect online businesses with real-time transaction-monitoring, passive detection of fraudulent activities, behavioral understanding of transaction patterns and non-invasive, user-notification methods

Entrust TransactionGuard provides real-time fraud detection and comprehensive fraud analytics. This proven solution is ready for rapid deployment using a zero-touch approach that requires no invasive integration with existing banking applications and does not impact the customer experience.

Entrust TransactionGuard transparently monitors user behavior to identify anomalies and then calculates the risk associated with a particular transaction — all seamlessly and in real time. Unlike competitive offerings, Entrust TransactionGuard can analyze all points of interaction with the user on the Web site with a zero-touch approach, allowing organizations to get a complete picture of potentially fraudulent behavior.

Using customizable, pre-built fraud rules and business signatures that describe a particular transaction path, the solution can help identify anomalies such as: a user login from an unknown machine; a login from a risky IP address or location; a transfer of unusually large amounts to unknown accounts; or a change of personal information.

Figure 3: Entrust TransactionGuard — Zero-Touch Fraud Detection & Analysis



Entrust TransactionGuard dynamically learns user behaviors and patterns, enabling the organizations to adapt to new instances of fraud without having to change a thing. The solution can also rapidly download and implement the latest defense against new behaviors from the Entrust Open Fraud Intelligence Network. All analysis is done transparently, rapidly and does not require the application to be changed in any way or cause extra burden on the user. Reporting tools mine rich data sets and can help deliver key information to the right users in a timely manner.

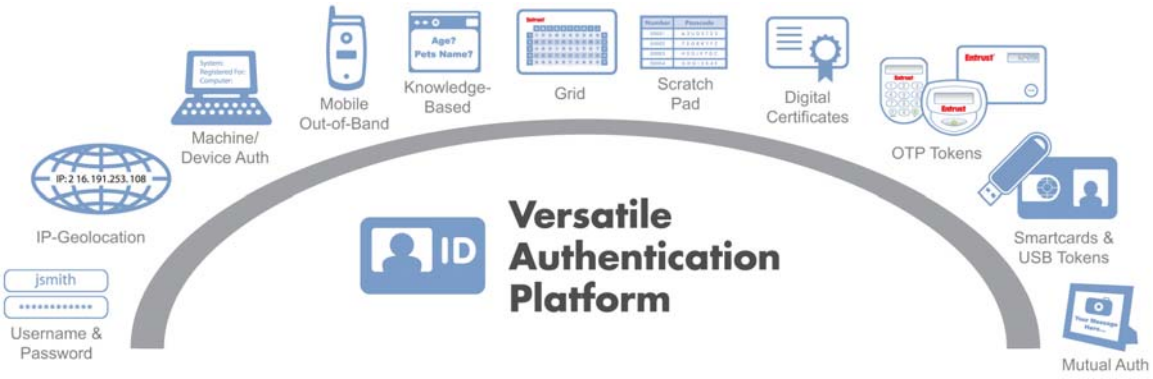
Importantly, Entrust TransactionGuard can be deployed in conjunction with not only Entrust solutions, but also additional third-party fraud offerings, delivering significant value to organizations looking to evaluate and understand all aspects of their online channel.

In combination with products like Entrust IdentityGuard, it can provide organizations with a comprehensive and cost-effective online security solution. In fact, Entrust has been recognized by Gartner as a "leader" in the recent Gartner Magic Quadrant for Web Fraud Detection (*see Section 8*) and is proven in some of the largest banks and financial institutions around the world.

Versatile Authentication Platform: Entrust IdentityGuard

Entrust IdentityGuard is the authentication solution of choice for some of the world's leading financial institutions. Serving as a versatile authentication platform, it provides a range of strong authentication capabilities for improved confidence for both parties in an online transaction. These capabilities provide organizations the flexibility to help match the risk associated with the given transaction to the proper strength of authentication.

Figure 4: Strong Authentication Options



Entrust IdentityGuard provides a range of easy-to-understand authentication methods that have minimal impact on the user experience. Personalized and mutual authentication accelerates user acceptance and can help increase deployment success.

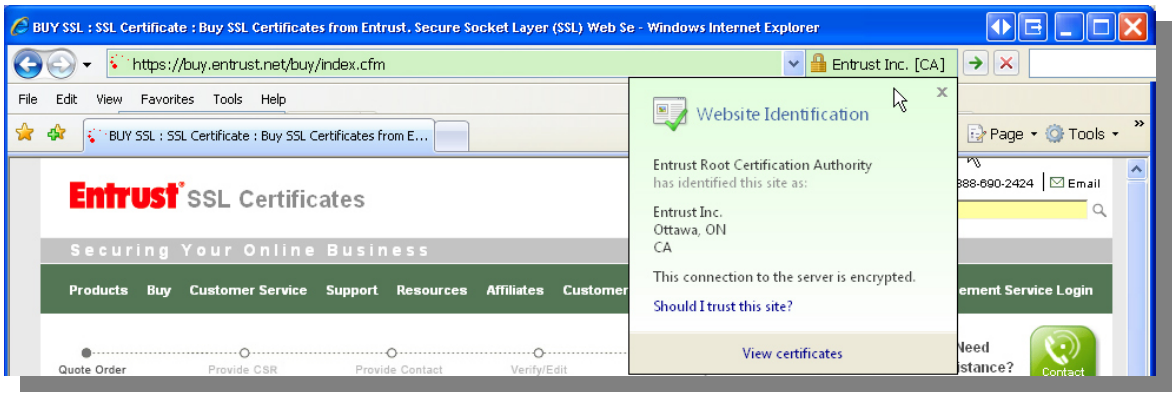
The platform offers a single point of administration, allowing easy implementation into existing processes. Entrust IdentityGuard can layer on top of existing password infrastructures and can leverage current fraud detection capabilities, helping provide a low-risk deployment that can be completed in situations involving tight timelines. Integrated with leading enterprise-class applications, Entrust IdentityGuard leverages its standards-based approach to deployment to easily fit into any enterprise infrastructure.

Next-Generation SSL Certificates: Entrust Certificate Services

A natural complement to Entrust IdentityGuard, Entrust Extended Validation SSL Certificates — commonly known as "EV" certificates — contain safeguards to help prevent fraud attacks (*see Figure 5*).

When consumers use an EV SSL-aware, next-generation browser, the technology will help users make smarter decisions of trust, such as the ability to verify the identity information of the owner of an EV certificate-protected Web site.

Figure 5: Extended validation (EV) SSL certificates provide a next-generation approach to addressing online attacks



8 Entrust a 'Leader' in Gartner Magic Quadrant

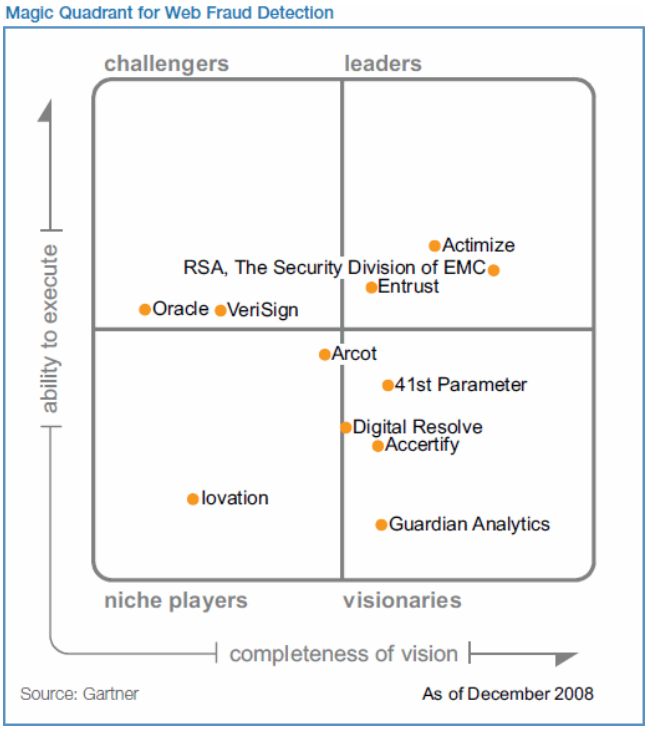
Even with heightened awareness, online fraud attacks continue to cost global organizations hundreds of millions of dollars each year.

As guidance in defining the major security experts who help prevent online fraud, Gartner offers comparative vendor research in the Magic Quadrant for Web Fraud Detection.

Gartner's Magic Quadrant for Web Fraud Detection named Entrust as a leader based on its "ability to execute" and the company's "completeness of vision."

Gartner defines leaders as: "Security vendors that have well-established records in fraud detection, achieving upward of 70 percent fraud detection with a false-positive rate of one to 10. (Some results have been much better.) They have earned high scores from many of their customers for responsiveness, effectively stopping fraud while minimizing inconvenience to their end users, and helping enterprise demonstrate a clear return on their investments.

"They also have full fraud detection feature sets, as well as sound road maps for future products and service features. They demonstrate a strong understanding of the marketplace, the ability to keep up with new fraud trends, and a commitment to staying in and winning in this market.



This Magic Quadrant graphic was published by Gartner, Inc., as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Entrust, Inc.

"They have also demonstrated that they can support markets in different parts of the world, other than their home country. Still, even these market leaders have much work to do in improving their products, services and customer support."[2]

Entrust's comprehensive strong authentication and fraud detection solution — comprised of Entrust TransactionGuard and Entrust IdentityGuard — helps many of the world's elite enterprises and financial institutions defend against online fraud, secure customer data and protect brand image.

[2] "Magic Quadrant for Web Fraud Detection," Avivah Litan, February 6, 2009, Gartner, Inc.

9 Conclusion

Multiple factors — regulatory compliance, advanced fraud technology, organized criminal elements, consumer perception and economic uncertainty — have forced today's organizations and financial institutions to adopt new technology to help combat online fraud.

The key lesson is that online fraud detection and prevention is an ongoing effort, requiring constant attention and investment. Thankfully, a handful of vendors today provide high-level solutions that are affordable, easy to use and non-invasive for end-users.

The following checklist will help serve as a baseline for next steps in evaluating fraud detection solutions. Critical considerations include:

- ☑ **Non-invasive deployment model** that allows you to quickly and cost-effectively deploy fraud detection across a broad range of financial applications
- ☑ **Real-time monitoring** of all transactions to stop fraud in its tracks
- ☑ **Blended approach to data analysis,** including both rules-based and statistical analysis, leveraging the benefits of both approaches
- ☑ **Comprehensive transaction monitoring,** including both front-door and in-session transaction details to maximize fraud detection capture rates
- ☑ **Risk-based authentication** that only prompts users for second-factor verification when really necessary, thereby providing the balance of security and positive user experience

Evaluating an organization's need and selecting the appropriate solution with a long-term strategy is the correct approach. Partner with a vendor who is an expert in online security, recognized as a leader in the industry and provides proven services and solutions.

With comprehensive buyer's guides and educational tools to help make the right decision for your consumer banking business, Entrust can help guide you along the way.

10 About Entrust

Entrust provides trusted solutions that secure digital identities and information for enterprises and governments in 2,000 organizations spanning 60 countries. Offering trusted security for less, Entrust solutions represent the right balance between affordability, expertise and service. These include SSL, strong authentication, fraud detection, digital certificates and PKI. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.