



# Securing the Enterprise Payments Network

VeriSign® Fraud Protection Services



## CONTENTS

Executive Summary	3
Fraud on Payments Networks	4
Payments Fraud Solutions	6
Deployment of Intelligence and Control	9
Conclusion	14

## Executive Summary

Among the technology assets that an enterprise owns, few are as critical to cash flow as the payments processing network. The payments infrastructure is the core conduit for managing a financial transaction from its origin with a customer sale, to its end destination in a business bank account. As this transaction flows through the enterprise network, it will be subjected to multiple business processes:

- Payment Authorization—Charge to a customer's payment tool to request collection of funds.
- Risk Screening—Assessment of transaction risk by automated technologies and the fraud or finance department. This may also include contact by customer service to validate order information.
- Fulfillment—Shipping of product by fulfillment department, notification to customer of order status.
- Settlement and Reconciliation—Finance request to banking networks for funds settlement between customer and enterprise bank accounts or reversal of transaction (void or credit).

Handling this transaction flow through the enterprise presents both security and operational efficiency challenges. How can a business scale its financial transaction volume without incurring undue risk exposure? How can a business put in controls on its financial transaction flows without burdening itself with operational and security costs? In short, how does an enterprise provide end to end security for this critical network?

Unfortunately, hackers understand that enterprises face a considerable task in addressing these challenges. They further recognize that compromising a business's payments system is the fastest route to cash. International crime rings now routinely target the enterprise payments infrastructure, looking for vulnerabilities that enable them to steal cash from the system.

According to the FBI, financial fraud is the second largest category of hacking events on the Internet today. Meridien research estimates that the potential cost to enterprises of not investing in payments security could surpass \$15 billion in 2005 alone. It is therefore essential that enterprises view their payments network as a critical infrastructure that will either restrict growth and burden the enterprise with costs, or free it to drive revenues.

This paper addresses the benefits of deploying VeriSign's Intelligence and Control<sup>SM</sup> across an enterprise payments network. The benefits range far beyond safeguarding a business from downside economic loss. VeriSign Intelligence and Control services enable enterprises to scale their transaction volume, and therefore their business, with confidence. Furthermore, efficient payments security reduces overhead and management costs, thereby freeing the enterprise to focus resources on business goals.

## Fraud on Payments Networks

Broadly speaking, businesses deploy payments networks in order to collect funds from customers and settle those funds with their bank. Their payments platform is a conduit that handles funds through this process. Hackers recognize that within this flow of money through an enterprise, there are three key vulnerabilities in payments security:

**Stolen information vulnerability:** Customer payment information is widely available over the Internet. This information may be stolen directly from insecure databases run by businesses or payments infrastructure providers. The largest reported compromise of credit card information to date was through a payments processor that exposed an estimated 8 million credit cards to an international hacking ring. Payments information is also exchanged in hacker black markets where credit card, bank account and social security numbers are auctioned to the highest bidder. The FTC reports that an estimated 27 million Americans had their identities compromised in the past five years. The ultimate impact is that customer payment information cannot be trusted at face value. Businesses must validate customer information and monitor its use in order to protect themselves from fraudulent attacks.

**Brute force attack vulnerability:** The widespread computerization and networking of business processes has made payments systems susceptible to a particular form of hacking known as a brute force attack. Using this method, hackers leverage computing power to breach a system's security and directly access payments data, or execute financial transactions. Software programs shared in hacker chat rooms automate the process of cracking passwords as well as identifying where network configuration errors can provide backdoor access into a business's systems. Another scheme known as "carding" leverages computers to launch a wave of purchase attempts that randomly guess for valid credit card numbers. If the appropriate security is not in place, this brute force process of guessing numbers will ultimately result in a valid match—the system is tricked into validating real customer information. The brute force vulnerability requires businesses to put effective real-time monitoring solutions in place so that automated attacks are quickly identified and blocked before they do any damage.

**Insider vulnerability:** While brute force attacks represent classic hack attempts to breach a network from the outside, the insider threat is much more direct. The same drive for business efficiencies that lead an enterprise to network its internal operations also makes customer information widely accessible to employees. Most customer service departments can access a wealth of data through CRM platforms. An insider granted privileged access, or an employee who abuses access privileges, can easily view vast amounts of sensitive payments information.

In a recent study by Harris Interactive, close to 50% of employees with access to customer information said it would be easy to view and download this information without detection. The insider threat is particularly damaging because most enterprises design security exclusively for external attacks. Without the proper internal controls in place, a trusted insider has free reign to abuse a financial transaction as it flows through the enterprise.

As an enterprise grows its business and puts increasing load on its transaction platform, it becomes more susceptible to these vulnerabilities. Hackers recognize this fact and have designed fraud schemes tailored to abuse them. While payments fraud schemes rapidly evolve with new technology innovations, they can broadly be bucketed into three categories of attack: Product theft, Identity theft, and Cash theft. An enterprise must secure itself against all three.

**Product Theft:** Product theft, also known as virtual shop lifting, is the most widely recognized form of payments fraud. Hackers use the widespread availability of stolen payments information to pass through fraudulent purchases under the cover of legitimate customer identities. When a payments tool is fraudulently used for a purchase, the banking industry holds businesses liable for the transaction by issuing a chargeback that requires businesses to return the funds. Since the average chargeback is not issued until well over a month after the purchase, hackers have plenty of time to commit the crime before it is discovered.

Most enterprises protect themselves from product theft reactively—they build lists of past fraud events and block future business with customers using those identities. While this is an important step in securing a payments network, it unfortunately does not protect the enterprise from immediate loss. It simply ensures the event will not happen again. Some enterprises take a proactive approach and mine their historical fraud data for patterns that might indicate future fraudulent attempts. While this may decrease fraudulent events, it may also inaccurately categorize fraud and simultaneously decrease sales. Gartner estimates that a business incorrectly rejects up to 3% of customer purchases during the risk screening process. For a company with \$100 million in sales this represents a \$3 million loss. Accurately screening risk indicators requires a massive scope of insight into transaction activity. Without this intelligence, a business is more likely to restrict growth than to support it.

**Identity Theft:** An enterprise's Web operations enable business transactions to occur 24x7 with anyone anywhere in the world. This convenience enables an enterprise to greatly expand its sales scope and drive top line growth. It also requires that the enterprise expose its transaction processing assets to a global audience. Identity theft is the primary goal of brute force attacks against these transaction assets. As discussed above, this may involve password cracking attempts to gain root access to a business's payments system (business identity theft) or carding attacks to validate credit card information (consumer identity theft).

Many enterprises do not plan for systematic attacks against their payments platform. But a well executed carding scheme can rack up thousands of dollars in losses in a matter of hours. Enterprises with widely recognized brands and high transaction processing volumes are more likely to be targets of these attacks. Hackers recognize that the system was designed to handle heavy transaction load—hence the effectiveness of automated random guessing. But any attempt to restrict access to payments processing also directly impacts the volume of sales that a business can complete.

Brute force attacks can only be repelled by intelligent velocity checks—real time monitoring of the transaction load on a network. Intelligent velocity checking not only analyzes the actual processing volume, it further analyzes the source and content of transactions. This method of checking provides maximum flexibility in responding to an attack, while ensuring that legitimate sales go through. Given that these attacks are targeted directly at the payments network, it is essential that this intelligence be as integrated into the payments platform as possible.

**Cash Theft:** Anyone with privileged access to a payments platform holds the keys to an enterprise's bank account. From this position of power, the individual can control the flow of funds through and outside of the business. Cash theft is by far the most damaging method of payments fraud that strikes businesses today. This method is commonly executed by organized crime rings that target the settlement and reversal of transactions. Hackers who can gain privileged access to a business's payments platform have the ability to run transactions on behalf of that business. A common scheme is to run a high volume of payments transactions against stolen customer payment tools, and then to credit or redirect settlement of those funds to the hacker's account. Given that this scheme is often undertaken by organized criminal groups, the funds are either quickly settled to overseas banks (where recovery is especially difficult) or shuttled through a series of bank accounts until the trail is lost. Since cash theft targets the back end of the transaction lifecycle, most businesses do not plan security procedures to block them. Cash theft is also a fraud method frequently abused by insiders who have the ability to not only execute the transactions, but erase their audit trails from the system. Controls around the backend of the transaction lifecycle are therefore a key element in complete payments security.

### Payments Fraud Solutions

Given the known vulnerabilities of payments networks and the high financial gain in exploiting them, businesses need a robust and effective method to enforce end to end security. Hackers target inconsistencies in payments security coverage that arise when an enterprise does not adopt a holistic approach. A holistic approach requires visibility into the entire transaction lifecycle (from funds collection through settlement), access to the widest spectrum of information to give them intelligence about transaction risk, and total control over funds movement through each stage of the transaction lifecycle.

**Visibility into the transaction lifecycle:** Most businesses dedicate the brunt of their security posture to reactive screening of transactions that come through the point of sale. The goal is to validate whether or not a customer’s purchase is legitimate. While this is certainly an essential part of securing the process it is insufficient on its own. There are two weaknesses to this approach when taken as the sole method of payments security. First, the reactive focus on validating completed customer orders does not proactively address real time brute force attacks. A hacker who wishes to validate payment information through carding does not care whether or not the order is fulfilled. The crime is often automated and completed within hours or minutes. By the time a risk management team has identified a fraudulent attempt, the business may have incurred extensive costs in authorizing transactions. In addition, the business now has a significant customer service burden in contacting legitimate cardholders to inform them of the security breach.

Second, a front end purchase screening approach does not address potential vulnerabilities downstream that are the focus of cash theft. System vulnerabilities such as external or internal access to processing privileges can go around the transaction screening process. The ability to trace financial events all the way through the system to bank settlement is the only way to ensure complete security coverage.

Below is a diagram of a payments security intelligence and control system that provides complete transparency into the lifecycle.

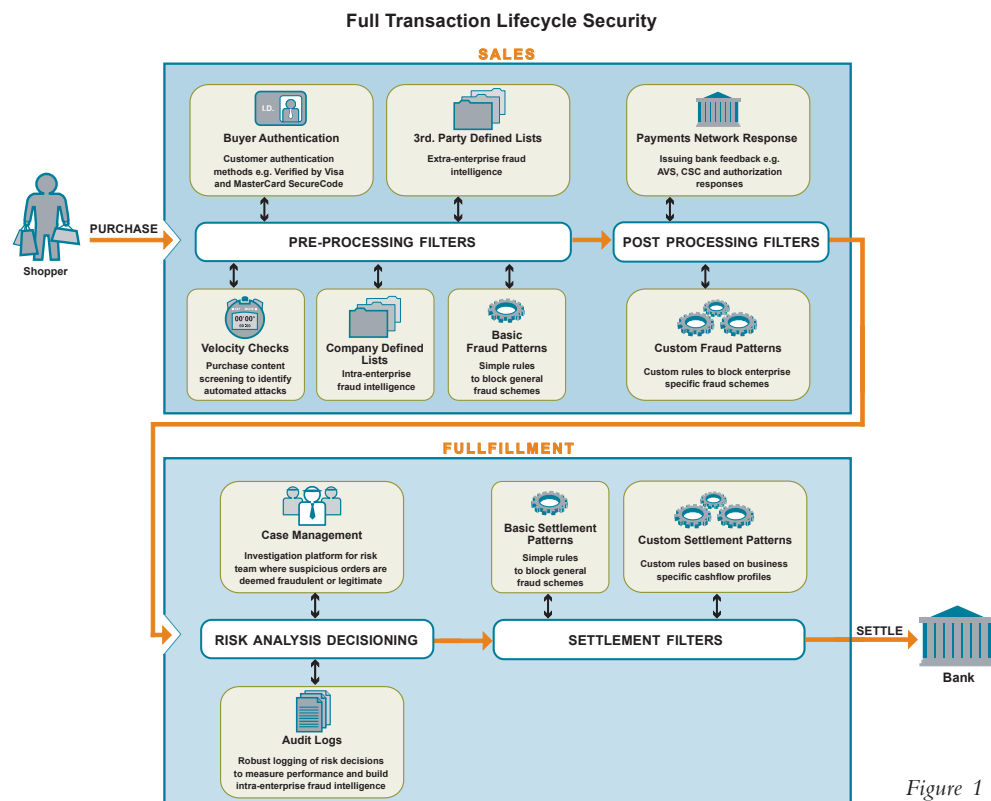


Figure 1

In the previous diagram, a payments transaction is fully screened to check for brute force attacks, authenticate the consumer, assess risk indicators, and escalate transactions for finance review. Then it is monitored through the fulfillment and settlement process. These stages will be further discussed in the “Deployment of Intelligence and Control” section.

**Access to Widest Spectrum of Information:** All businesses have access to a robust suite of internal information to enable real time security intelligence. But typically this does not provide sufficient scale or visibility into the reality of payments fraud on the Internet. True security intelligence is derived across three horizons: within a single enterprise network, across multiple enterprises and across the Internet. Practically speaking, businesses do not have the resources to pursue intelligence beyond their own payments systems. Finding a strong payments security partner is important to achieving this end.

As a provider of Internet infrastructure services VeriSign has unique visibility into security patterns, trends and threats across the Internet. VeriSign owns and operates eight state-of-art data centers and 13 top-level domains constellation sites throughout the world. Through this infrastructure, VeriSign resolves over nine billion domain name system look up transactions a day, secures nearly 400,000 Web sites and processes close to 30% of all U.S. e-commerce transactions. Beyond having this visibility, VeriSign has deployed a world class fraud operations center where the broad range of payments data it handles can be correlated to rapidly identify emerging threats. VeriSign’s proprietary intelligence on sources of Internet fraud helps it to distinguish serious hackers, from script kiddies, to internal fraud threats. The fraud operations center provides a tiered support structure where trained risk analysts monitor all payments events through the system. Enterprises leveraging the VeriSign Fraud Protection Services have access to one of the broadest databases of fraud patterns available today.

**Control Over the Transaction Lifecycle:** Transparency and intelligence provide the final value to businesses in securing their payments network against fraud—complete control over the transaction at every stage in its lifecycle. Figure 1 illustrates a system in which control is maintained at every point as the transaction progresses from funds collection to settlement. At any point within this path that a suspicious event occurs, the appropriate decision makers can be alerted to take action before the transaction continues. Oversight of the lifecycle can be managed in its totality by one business group with clear responsibility for the enterprise’s risk exposure. The ability to define clear owners combats one of the greatest vulnerabilities in any complex system—the lack of individual accountability for outcomes. When one group bears responsibility for payments risk it enables quicker response times and more effective use of information. It also provides a clear path within the enterprise for employees that do not have this responsibility to escalate issues that require immediate resolution.

The end benefits of a payments security platform that provides intelligence and control are extensive. Businesses with greater insight into the risk of a transaction are free to extend their sales channels and thereby increase total commerce volume and revenues. With the appropriate controls in place, businesses not only reduce their exposure and potential economic loss, they further increase their overall efficiency. Efficient allocation of resources reduces the costs of security while simultaneously ensuring best in class security standards. This frees resources within the enterprise to focus on strategically differentiating projects like effective marketing campaigns and better customer servicing.

As part of VeriSign's Intelligence and Control services suite, it now offers the VeriSign Fraud Protection Services for enterprise payments platforms. The remainder of this paper will take a more granular look at how businesses can deploy this offering to secure their business.

### Deployment of Intelligence and Control

A common concern for businesses when deploying a security system is how to increase security without hampering flexibility and slowing down internal operations. Enterprises fear trapping themselves within a fortress that inhibits their freedom to grow. The VeriSign Fraud Protection Services was designed to provide the maximum amount of intelligence and control while ensuring that financial transactions flow efficiently through their entire lifecycle. The system was designed based on VeriSign's own need to maximize security within an operational environment that handles over 1 million transactions a day and \$20 billion annually. The only way to ensure performance at these levels was to build a system from the ground up based on a stringent set of business criteria. VeriSign set the following design requirements for the VeriSign Fraud Protection Services:

**Never disrupt the natural transaction flow:** Any risk service that disrupts the natural flow of a transaction does a disservice to an enterprise's key objective of closing sales. Disruption can occur in multiple forms. Time delays in transaction screening can "time out", resulting in network errors or customer abandonment. Excessive false positives hold up the fulfillment of legitimate customer purchases. Cumbersome response codes weigh down the transaction with data and increase the likelihood it will conflict with other enterprise systems. To ensure that every legitimate transaction flows efficiently through the system, VeriSign took a number of steps.

First, it built a horizontally scalable system that can handle massive transaction volumes at minimal response times. This formidable processing power ensures that transaction screening will not time out or lead to customer abandonment. Second, it provides a battery of screening logic fully customizable by risk departments to rapidly hone in on only the most suspicious transactions. This screening logic can be set to observe mode (where it only reports on the transaction without taking action) or active mode (where transaction control is put in place and purchases are denied or escalated for review). The observe and active modes enable an enterprise to ease in security controls without committing to a path that might disrupt the natural flow. Third, it enables enterprises to dial up or down the verbosity of data feedback on a transaction. Feedback can be stripped down to basic levels that do not encumber the system with additional responses, or made robust to push the greatest amount of information back to the enterprise. Fourth, VeriSign designed for extensive exception handling scenarios. In the event that any portion of the system fails the business is immediately alerted and all data is logged. The system even enables efficient recovery by providing offline re-screening of failed transactions to ensure that every financial event successfully passes through the risk system.

**Manage and leverage the enterprise's intelligence:** With VeriSign's extensive insight into fraud attacks, it was essential that fraud learnings could quickly be cycled back into the system. Leveraging the enterprise's intelligence enables a risk system to grow and evolve with experience. Learnings come both in the form of negative events (identified fraud cases) and positive events (identified legitimate customers). The VeriSign Fraud Protection Services enables an enterprise to store knowledge from these events within the system where it can easily be brought to bear on the fraud screening process. Risk departments can upload data associated with fraud attacks to ensure they are not replicated. Data associated with loyal repeat customers can also be brought to bear to ensure that legitimate purchasers are not blocked. Enterprises will also notice over time that certain product sets are more likely targets of fraud attempts than others. This information can also be loaded into the system in order to focus risk screening on the areas where it will have most impact.

In addition to building real time screening intelligence into the platform, the VeriSign Fraud Protection Services also provides tools for risk departments to manage overall risk learnings and assess system performance. All audit trails associated with both positive and negative events are stored in Web based reports accessible through the case management platform. These reports, along with analyst research notes, can be pulled by date range, transaction status, and risk decisioning outcome. Risk reports provide the CFO or other financial executive with real time insight into a business's cash flow risk. Since the banking networks can take 24 hours or longer to log transaction events, this provides the most immediate view into overall transaction security.

For a system performance view, additional reports indicate how many times each specific rule took action on a transaction. These reports can be used to gauge overall risk screening effectiveness and what impact the fraud screening system is having on the enterprise's financial transaction flows. The automated portion of risk screening can therefore easily be analyzed and modified to meet the enterprise's overall business goals.

**Enable rapid and cost effective deployment:** A unique quality of security technologies is that they must evolve more rapidly than other enterprise applications. Innovation is at the core of hacking methodology. Hackers probe enterprise systems in order to identify vulnerabilities that provide a path to their goals. Once these vulnerabilities are identified, the enterprise cannot wait for lengthy code roll outs to take action. Speed and flexibility are therefore at the heart of security. But both of these qualities come at a cost that directly impacts the Return on Investment (ROI) of any security system. If the cost of a security system exceeds the value of its protection, it immediately loses its utility.

VeriSign took a number of steps to ensure that the VeriSign Fraud Protection Service could be rapidly rolled out across a payments system with the fastest ROI and the least amount of engineering integration. The diagram below illustrates the first implementation of the VeriSign Fraud Protection Services on VeriSign's own Payflow transaction processing platform. A key design goal was to enable existing businesses using the Payflow technology to easily expand their existing integration to incorporate complete security intelligence and control. Businesses that use the existing Payflow Software Development Kit (SDK) simply have to expand the number of data fields they pass to the service in order to benefit from complete security coverage. For some customers this has meant as little as one day of integration and testing to ensure that additional information is passed in and security specific response codes are incorporated into their applications. The Payflow gateway is pre-integrated with the VeriSign Fraud Protection Services to handle all real-time screening, risk management oversight and control over the financial transaction flow through its various stages. All features can be managed through the existing VeriSign Manager application. This includes rules set-up, rules deployment, risk reporting, risk decisioning and settlement.

Enterprises can also manage daily transaction flows through their existing order fulfillment systems. The VeriSign Fraud Protection Services provides verbose fraud responses that allow employees at the company to pull risk related data into their enterprise platforms for review from their in-house risk management systems.

VeriSign handles all processing and risk management transactions within its 24x7 production environment to limit hardware and software requirements for the enterprise. Figure 2 illustrates the transaction flow for an enterprise integrated with the Payflow SDK.

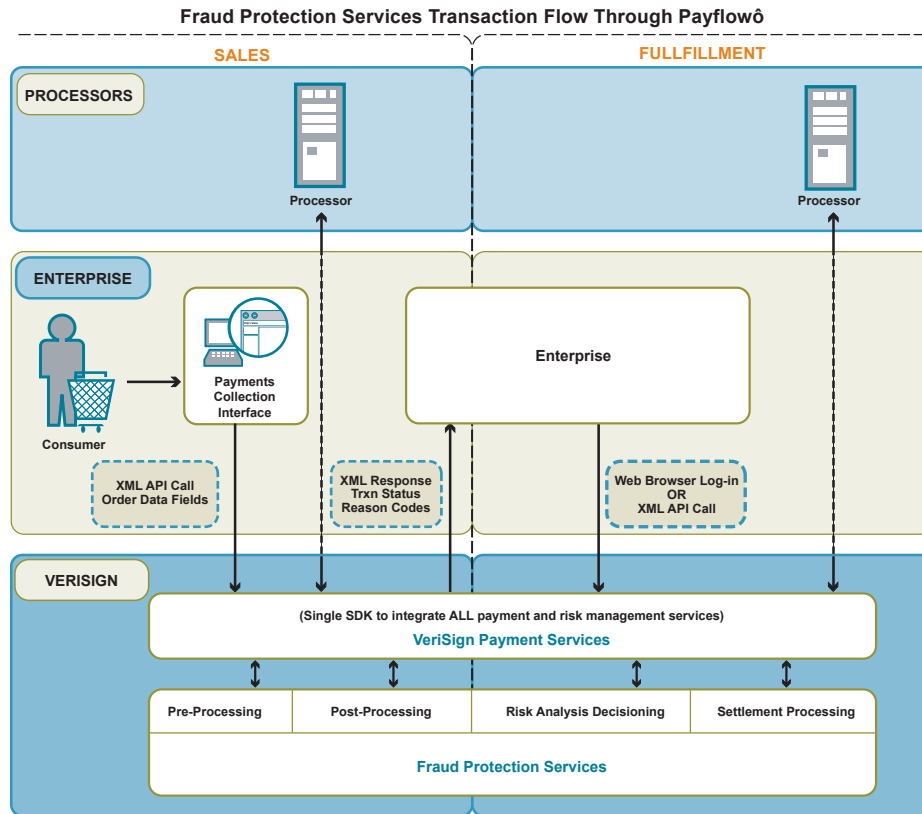


Figure 2

Businesses using the Payflow services need only to expand the XML call made to VeriSign with all the data fields relevant for screening the risk of a transaction. This may include passing additional fields such as customer IP address, already part of the Payflow SDK, that enable the fraud screening platform to perform velocity checks, geolocation screening and other filters to identify risk indicators in a transaction. The risk department logs into a Web based account in order to set-up and deploy screening logic. Risk analysis and decisioning can also be handled using the VeriSign Manager reporting and case management platform. If the enterprise already leverages an in-house reporting and case management platform, it also has the option to leverage the VeriSign Fraud Protection Service’s robust reason code responses to execute review and decisioning from its own systems. In this instance, an additional API call is necessary to manage the transaction status on the Payflow system.

**Provide a system that is easy to manage:** Usability is a key driver of any security system's effectiveness. If the system is too difficult to manage it will never be integrated into the enterprise's daily operations. Most payments security systems require extensive engineering support to be configured and managed on a daily basis. The result is that risk management frequently falls within the responsibility of the enterprise's IT group. When VeriSign built the VeriSign Fraud Protection Services it undertook extensive usability testing with risk management professionals to ensure that its system would be easy to deploy and manage by risk business owners. All risk screening rules can be built and deployed through an intuitive graphical user interface (GUI) that does not require engineering resources or code updates to roll out into production. Rules can be modified at any time and immediately be redeployed within the architecture. This guarantees both flexibility and autonomy for business risk analysts who need to make real time decisions about the enterprise's risk exposure. A test platform enables analysts to test the performance of rules before deploying them into the live processing environment. No professional services or consulting engagements are required to fully update the security system. The rules building GUI shortens the risk team's response time from weeks or months to under an hour.

**Grow with new technologies:** Finally, VeriSign recognizes that any payments security system must be modular in design to ensure its extensibility and growth over time. While the VeriSign Fraud Protection Services represents the most robust integration of payments security technologies in any platform, the technology for both fraud and fraud protection continually evolves over time. Visa and MasterCard recently launched buyer authentication programs (Verified by Visa and MasterCard SecureCode), but other card associations and financial institutions are likely to offer their own authentication programs in the future. The VeriSign Fraud Protection Services authentication module readily expands to incorporate these programs as they become available. Pattern matching technologies and risk lists are also expected to evolve over time as Internet fraud protection matures. As these technologies become available to increase the security intelligence and control over a payments system, they can easily be bolted onto the VeriSign Fraud Protection Services architecture. Figure 3 illustrates the VeriSign Fraud Protection System architecture and its modular design to quickly incorporate new technologies.

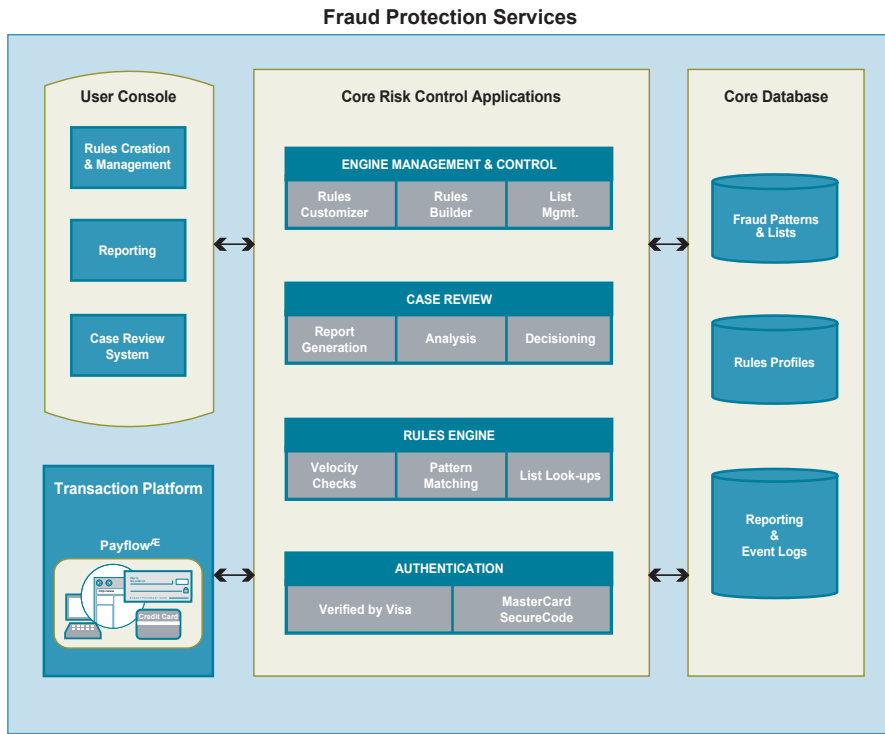


Figure 3

**Conclusion**

Enterprises that operate at large scale, or that intend to rapidly scale their sales channels, must view their payments platform as a critical technology asset to their business. As with any critical asset, effective security is a necessity to protecting the business and supporting its growth. The VeriSign Fraud Protection Services provides the most holistic intelligence and control available for an enterprise payments system today. But the benefits of intelligence and control range far beyond protection. Ultimately, it is essential to the enterprise’s overall business objectives. Contact VeriSign Payment Services at 650-426-5551 or [vps-enterprise@verisign.com](mailto:vps-enterprise@verisign.com) to learn more about how to benefit from this revolutionary new offering within the VeriSign Intelligence and Control services suite.