The Industrialization of Fraud Demands a Dynamic Intelligence-driven Response

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for RSA, the Security Division of EMC

October 2016

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary 1

Fraud in 2016: The Continuing Evolution of an Industry 1

Expansion of Mobile as a Platform and a Target for Fraud 4

The Net Result: The Industrialization of Fraud 4

How to Defend Against an Industry 7

Dynamic, Adaptive, and Intelligence-driven 8

RSA Fraud and Risk Intelligence Solutions 8

At the Core: Intelligence and Expertise 8

Integrating Real-time Intelligence With Anti-fraud Technologies 9

Pre-Access Protections 10

During-Authentication Protections 10

Post-Authentication Protections 11

EMA Perspective 12

About RSA 13

Executive Summary

As criminals discover the profitability of attacks against information systems, fraud has increased significantly with no end in sight. Adversaries learned the lucrative nature of harnessing cyber threats. Innovations now make it easier to steal from a wider range of victims, spurring the commercialization of multiple forms of crimeware and an entire Internet subculture known as the "Dark Web" or the "Dark Net," where both software and services can be rented or purchased. The Dark Net services gave rise to specialization, competitive pressures, and other factors that illustrate how fraud, abetted by cybercrime, grew from the unrelated activities of a few into an industry in its own right.

This industry produced a level of automation and sophistication in fraud techniques rivaling those of the legitimate business world. The commercial-grade packaging of complex threats makes it possible to readily convert personal systems into pawns that facilitate fraud, often unbeknownst to their rightful owners. Large-scale systems management capitalizes on the ability to harness entire networks of compromised hosts whose masters often avoid detection and eradication through highly nimble evasive tactics. The net result: an industrialized threat that costs businesses billions to trillions of dollars worldwide.

In this paper, Enterprise Management Associates™ (EMA®) explores the response organizations must marshal to stand up to the threat of industrialized cybercrime. If attackers are well organized and well informed, take advantage of the latest innovations in the shadow market of crimeware and automation, and capitalize on intelligence to maintain their advantage, organizations must respond accordingly.

Coordinated strategies embracing multiple tactics to limit exposure and improve effectiveness are now mandated by guidance such as that of the PCI Council, the US Federal Financial Institutions Examinations Council (FFIEC), and other regulations worldwide, affecting businesses targeted by fraud. The RSA Fraud and Risk Intelligence services portfolio offers an example of just such a coordinated approach. With its early leadership in technologies and services that integrate intelligence with anti-fraud tactics in real-time, the RSA Fraud and Risk Intelligence portfolio provides organizations with the tools to enable strategies for confronting an industrialized threat with an industry-wide response.

If attackers are well organized and well informed, take advantage of the latest innovations in the shadow market of crimeware and automation, and capitalize on intelligence to maintain their advantage, organizations must respond accordingly.

Fraud in 2016: The Continuing Evolution of an Industry

In years past, attackers who sought to perpetrate fraud by exploiting information systems often worked alone. They selected their methods, harvested valuable data, and carried out fraudulent transactions in relative isolation, working independently for their own gain.

Today, the profitability of cybercrime transformed the nature of the game. Consider phishing attacks alone, which the RSA Anti-fraud Command Center (AFCC) estimates to have cost businesses over $2.17 billion in global fraud losses in 2015.[1] Phishing continues to be a problem that plagues businesses around the globe. According to the Anti-phishing Working Group, the number of brands hijacked by phishing campaigns grew by over 250% in 1Q16 to over 1200 affected brands. This exceeded

[1] http://www.emc.com/microsites/rsa/phishing/index.htm

any other three-month span since it began tracking the issue.[2] The retail/service sector was the most targeted, receiving almost 43% of the attacks, followed by the financial sector with nearly 19%, and the payments sector with just under 15% of the attacks, making the top three industries the target of over 75% of the phishing attacks.[3]

Growth and profitability had the same impact on the business of fraud as they would in any other endeavor. They created a market as well-defined as any in the legitimate business world:

- **Commercialization:** From assortments of exploits collected over time and through the experience of individuals, the profitability of fraud has matured attacks into packaged products and even product sets made available through covert commercial channels. Frameworks that enable exploits to be built from components accelerated the "time to market" of more complex threats, exhibiting a sophistication in serving a market that directly parallels legitimate software businesses.

  These threat packages continue to evolve; most notably, in 2015 the availability of exploit kits and anti-forensic mechanisms exploded. Packages named Angler, Nuclear, Magnitude, and Rig were the most active kits available from Dark Net vendors. Techniques such as upgraded URL pattern changes, landing page redirection using steganographic engines, and focused JavaScript all targeted landing page entrapment techniques.[4]

  Distributed Denial of Service (DDoS) capability became another popular feature of commercial crimeware, capitalizing on highly distributed threat networks (such as botnets) to turn compromised hosts into DDoS amplifiers on an enormous scale. Since late 2012, banks are increasingly targeted from such attacks, capitalizing on DNS system vulnerabilities and web servers compromised by crimeware tools such as "itsoknoproblembro." DDoS attacks have thus far culminated in September 2016 with the largest volumetric DDoS attack in history. The attack was reported at 620 Gbps and was against noted security journalist Brian Krebs' website.[5]

- **Commoditization:** The expertise of a few has become available to many. Once an attack concept becomes coded as malware, it becomes available to a greater number of adversaries who need not be more sophisticated than the original author (and are often far less). As the tools of fraud became more widely available, prices fell accordingly. In 2013, remote access tools sold for between $50 and $250. In 2016, they are selling for $5.[6] This commoditization, however, came at a cost to the criminal. Penetration, prosecution, and disruption of such widespread and highly visible activity by law enforcement and anti-fraud efforts led some crimeware organizations to privatize their operations by restricting access to outsiders and, in some cases, taking commercial offerings off more open markets. The increased demand may result in upward pricing pressures.

- **Competition:** Additional pressure is placed on criminals as more competitors and attack platforms enter, or re-enter, the market. The SpyEye Malware, for example, became a significant competitor to Zeus, actually displacing it when found on a target. Since 2013 extortion attacks have been on the rise, especially those based on ransomware. In early 2016, numerous hospitals, local governments, and large enterprises had data captured by ransomware. Because of the early success of CryptoLocker, numerous competitors such as CryptoWall, Cryptodefence, Locky, and Samas are now competing for distribution and ransom dollars, with the average demand about $300 for individual machines.[7] If the ransomware is "lucky" enough to capture critical business systems or a large number of systems, the fees are much higher.

[2] http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf
[3] Ibid.
[4] https://www.sonicwall.com/whitepaper/2016-dell-security-annual-threat-report8107907/ page 3
[5] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[6] Dell SecureWorks Hacker Underground reports 2013 and 2016 editions
[7] Institute for Critical Infrastructure Technology

- **Specialization:** Market pressures and new opportunities also led criminals to add specialized features to attack platforms, including not only multiple packaging options for code obfuscation, but also specialized/focused operating systems and application options for targeted delivery. Criminals are also becoming more industry-focused to provide a higher return for their customers in their specialization area. Criminal solutions providers also expanded into mobile. Variants of many popular attack packages such as Citadel, Zeus, SpyEye, and Carberp can now be equipped with malicious mobile apps that can intercept and forward the SMS messages often used to transmit one-time authentication codes – likely heralds of significantly increased fraudster investment in mobile threats to come. As of 2016, 60% of fraudulent transactions originated from the mobile channel.[8] Meanwhile, geographic-specific malware continues to advance as a trend, recognizing that different language and cultural regions may require their own distinct authentication and attack techniques in order to be effective. Supplemental "off the shelf" products arose to serve emerging segments of the market, such as "anti-security" software that defends crimeware against detection and defeat.

- **Fraud as a Service:** The increasing specialization of fraud also gave rise to entrepreneurs who recognize the value of services to support and enhance fraud activity. The landscape of Fraud-as-a-Service has evolved. In the past, malware purveyors offered what are effectively subscription services where providers made remote access toolkit (RATs) support services, including the setup of the C2 server and aid in infecting the victim available for incremental fees, or providing unlimited access to a variety of modules for $50 per month.[9] The increased pressure on criminals to limit the availability of fraud tools and services, privatize their operations, and "play closer to the vest" created more service segmentation and/or a broader range of focused providers and groups of specialized criminals. These groups worked together to deliver a broader portfolio in a single portal to increase their customer appeal. Since 2013, researchers have been seeing Dark Net providers emulating cloud SaaS models and delivering cybercrime platforms supporting plugins, exploit kits, and administrative consoles. These platforms increase overall revenue by leasing access to tools and resources monthly rather than selling them outright. Botnet setup and support services remain in high demand, with bundled deals of malware binaries combined with hosting on hardened servers, encryption, plugin sets, and web injection packages. Criminals even offer cybercrime training for less skilled fraudsters. An industrial scale example of this is the commercialization of Sentry MBA services. Sentry MBA is used for automated account checking to locate credential reuse across the Internet. Since 2014 and the mega-breaches of billions of email accounts, the Sentry MBA as service offerings increased dramatically. In 2016, they were fully commercialized with a range of services including custom seed files, implementation support, hosting for scanning and, of course, customer support if the attacker has any problems getting his/her campaign off the ground.

The increasing specialization of fraud also gave rise to entrepreneurs who recognize the value of services to support and enhance fraud activity.

[8] RSA Adaptive Authentication Core Risk Engine
[9] https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

Expansion of Mobile as a Platform and a Target for Fraud

In discussing the state of fraud as an industry in 2016, the expanding use of mobile platforms must not be ignored. Mobile is both an expanding platform for conducting fraud and a large target of fraud. In 2015, half of all online purchases made on Black Friday were with mobile devices. This fact shows the increased adoption of mobile as a payment platform based on the convenience mobile devices bring to consumers' lives. It also means a lucrative opportunity for cybercriminals since the mobile channel is perceived as the less-protected digital channel. Last year, RSA saw that mobile traffic represented about 45% of all transactions, and 60% of fraudulent transactions originated from a mobile device.

As a target of fraud, mobile users and devices are subject to attack from malware and fake mobile apps designed to collect user credentials and account information. A recent study identified that while 87% of merchants supported mobile transactions, only 62% of them could truly determine whether the transaction originator was actually a mobile device.[10]

The lack of visibility into traffic, as well as the escalating fraud problem, is driving the need for a new breed of technologies to protect the mobile channel. One of the fastest-growing second factors of authentication are biometrics, the use of biological traits such as fingerprints, irises, retinal patterns, and circulatory system patterns to uniquely identify a user. Users see this commonly with fingerprint ID on smartphones for access and utilizing various electronic payment systems such as Apple Pay, Samsung Pay, and Google Wallet. Biometric authentication is highly leveraged with these mobile payment schemes to harden them against account takeover via device theft.

The lack of visibility into traffic, as well as the escalating fraud problem, is driving the need for a new breed of technologies to protect the mobile channel... both the skill and monetary barriers of entering the "hacking" business are considerably lower.

The Net Result: The Industrialization of Fraud

These developments make one central fact clear: fraud evolved from a criminal engaged in activity into a criminal industry. In the most recent email metrics report of the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG), spam and messages that abuse email systems made up 90.2% of mail volume across more than 400 million mailboxes among the participating member service operators.[11] That is a steady increase across 2015, culminating in Q1 2016 with a 4x increase in messages with malicious attachments over the same period in 2015.[12] Much of that malware targeted fraud as its objective.

How were malicious threat actors able to dominate this much legitimate IT? Through the sophistication of attacks made possible by an industrial ecosystem:

- *Reduction in barriers to entry* is one of the first and most prominent outcomes of industrializing the ecosystem. Previously, those who wish to participate had to build skills and tools, which was time consuming and/or costly. Fraudsters leverage multiple avenues from the Dark Net to open forums across popular social media sites, now providing marketplaces for hacking tools, tips, and education. Both the skill and monetary barriers of entering the "hacking" business are considerably lower. Malware development and packing platforms, botnet warehouses, DDoS services, stolen

[10] http://info.kount.com/mobile-payments-report-2016
[11] https://www.m3aawg.org/sites/default/files/document/M3AAWG_2012-2014Q2_Spam_Metrics_Report16.pdf
[12] https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/

accounts, and more are all for sale at very reasonable rates. Much of what was formerly a tradecraft, grown and nurtured through years of work, can now be had for a small service fee that includes documentation and training.

- *Multifunctional attacks* that encompass a variety of ways to compromise victims were made possible by readily-used frameworks for their construction, and crimeware of a quality similar to commercial-grade off-the-shelf software in packaging, delivery, and support.
- *Sophisticated automation* rivals the scale and efficiency of enterprise-class IT management systems that enable the fluid control of large-scale networks of compromised hosts.
- *Tools* harness the power of the Internet to further expand fraud on a similarly global scale. For example, compromised hosts can become spam or phishing amplifiers, dramatically decreasing the likelihood of successful detection and increasing the likelihood of successful exploit.
- *Exploited and Malicious Websites* are malicious as well as legitimate sites whose vulnerabilities were exploited and are leveraged to further propagate attacks by enabling a compromised host to download additional crimeware at the command of a remote manipulator, often without the victim's knowledge. The reach of sites can be further extended through techniques such as search engine manipulation.
- *Human Exploitation and Social Engineering are* used to engage people in the fraud process. People in third-world or other very low income areas often perform often straightforward yet lucrative tasks such as cross-border money transfers, ATM and in-store card fraud, and overcoming web-based human detection such as CAPTCHA, check boxes, and logic problems that must be solved to access a site. These human operators use various forms of social engineering to operate against the people in the control chains and execute against end consumers.
- *Asset Control* is a key strategy for Fraudsters and businesses. Just as mature businesses do, fraudsters monitor their personnel for individual theft (skimming) of profits, attempts to leave the organization, or reporting activities to the police. They also maintain inventory of compromised endpoints and websites, tools, and other software resources, and inventories of what IP address ranges they already attempted to compromise for work efficiency.

At this industrial level, fraud becomes an efficient business of opportunity. Each one of millions of compromised victims can become a source of information that can be exploited to siphon off material assets – or perhaps to access even more valuable data, such as intellectual property or other assets whose compromise could seriously damage a victim – regardless of whether it is an individual or global enterprise.

The tactics of industrialized fraud give criminals access to a wide range of targets, from the usernames and passwords of legitimate account holders, to personal data that enables fraudsters to successfully impersonate victims in applying for credit or access to tangible assets. These lead to account takeover and the creation of thousands to millions of fraudulent accounts. This is especially prevalent more recently, with the breach of more than 1.5 billion usernames and passwords across many popular consumer websites in 2016. The breach of account data at one location also leads to other companies being victims of account fraud via takeover because of account IDs and passwords recycling on the part of users.

Access alone is not the only risk. Once access is gained, organizations must maintain vigilance over transactions to assure that access was not gained through fraud, or that fraud is not the objective of what appears to be legitimate access.

> **Access alone is not the only risk. Once access is gained, organizations must maintain vigilance over transactions to assure that access was not gained through fraud, or that fraud is not the objective of what appears to be legitimate access.**

This, in turn, indicates the level of intelligence defenders must muster to match the intelligence capabilities of criminals in control of millions of compromised victims. These professionals are able to evade detection through nimble techniques such as the ability to move command and control (C2) services quickly from one mass of bots or botnets to another, or to hide behind complex abstractions of IP addresses, hostnames, and domains that change dynamically in response to attempts to detect and expose fraud activity.

Given these capabilities, it is hardly surprising that industrialized cybercrime rivals even the greatest achievements of legitimate efforts. Large-scale botnets, which included the likes of Conficker, Mariposa, ZeroAccess, Metulji, and GameOver Zeus, controlled as many as 50 million Internet hosts, generating over 90% of the world's SPAM messages, perpetrating advertisement click fraud, being leveraged for worldwide DDoS disruptions, and operating as a major source of ransomware distribution and control.[13] Ransomware alone collected at least $209 million in the first quarter of 2016 and FBI estimates project that it will reach upward of $1billion in 2016.[14] Estimates indicate 2019 cyber fraud could reach as much as $2 trillion,[15] rivaling the GDP of India, which ranked 7th in the list of national GDPs.

These facts describe the nature of concern manifested in guidance issued in 2014 by the US Federal Financial Institutions Examinations Council (FFIEC) in its Cybersecurity Assessment General Observations, which noted updated best practices such as:

- Routinely discuss cybersecurity issues in meetings
- Monitor and maintain sufficient awareness of threats and vulnerabilities throughout the organization
- Establish and maintain a dynamic control environment
- Manage connections with and to third parties
- Develop and test business continuity and disaster recovery plans that incorporate cyber-incident scenarios[16]

These concerns are shared by regulators worldwide, including the Reserve Bank of India, European Banking Authority, South Korea's Financial Supervisory Service, the Infocomm Development Authority of Singapore, Mexico's National Banking and Securities Commission, and the People's Bank of China – all of which responded since early 2010 with regulations targeting many of the same objectives as the guidance of the US FFIEC.

This concern extends beyond financial fraud alone. It should be noted that once criminals have access to sensitive data linked to tangible assets, they might not stop at fraud. The access to additional sensitive information made possible by the tactics of industrialized fraud – such as usernames, passwords, access information, sensitive intellectual property, or other valuable information assets – could be exploited to commit other crimes, which could cause even greater problems for individuals and organizations alike.

[13] http://www.gfi.com/blog/bad-botnet-bad-the-12-worst-botnets-of-the-past-decade/
[14] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[15] http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#2a77bf5f3bb0
[16] http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf

How to Defend Against an Industry

Strategists should take note of the common themes in these aspects of industrialized fraud:

- **An industry enables efficient, large-scale operations.** Sophisticated automation backed by integrated capabilities from multiple sources speaks to how the fraud landscape has matured. Global complexity is managed deftly when the tools of industry make it possible.
- **Broad intelligence capabilities inform and refine fraud techniques and drive further evolution of the fraud industry.** Using large-scale automation, criminals collect intelligence from successful as well as unsuccessful exploits across millions of victims, enabling them to identify common weaknesses to tune the most successful tactics for evading fraud defenses to achieve a successful campaign.
- **Controlling identity is key to successful fraud.** Fraud, after all, is about exploiting access to, and control over, valuable assets, and the technologies that handle them. What many organizations may have overlooked in the growing industrialization of fraud, however, is that protecting identity has come to mean much more than just strengthening a login or password. Today, it means greater protection for both individuals and institutions, and not just at login. It is vital to assure identity in the access provisioning phase through system/application access and into validating legitimate activity throughout transaction processes to defend transactions against abuse. Identity has become a critical factor in protecting organizations from fraud risk. This also highlights the pivotal role of identity in a "layered" approach to security, such as that described by the US FFIEC.

Identity has become a critical factor in protecting organizations from fraud risk...without swift and concise response capabilities, it is impossible to construct and maintain effective detection and defense.

Defenders must respond accordingly:

- **Harnessing dynamic intelligence is vital.** Today, intelligence, detection, and defense are coming together as never before. Defenders must have broad as well as detailed insight into activity across the fraud landscape – but this means more than just awareness. Today's most advanced techniques for protecting assets harness that intelligence in real-time, from equipping expert anti-fraud analyst teams with up-to-the-moment insight, to automating the decision to permit, block, or more closely monitor transactions when evidence of potential or actual fraud is found. Today, the application of new technologies that optimize behavioral analytics across large and dynamic bodies of data opened new vistas to fraud analysts and real-time defense alike.
- **Combating an industry requires a response up to the task.** Once the foundation for information collection and analysis is created, response automation and well-documented processes must be in place. Without swift and concise response capabilities, it is impossible to construct and maintain effective detection and defense.
- **Controlling identity is key for stopping fraud.** If fraud is about exploiting access to and control over valuable assets, defending identity and strengthening authentication is then paramount to defeating fraud. Fusing a risk-based approach with identity and access management creates an entirely new intelligence-driven defense for defending against unauthorized or criminal access. It means arming identity and access management with a dynamic, intelligence-driven response to attempted fraud, from the outer defenses of application systems through the lifecycles of sensitive transactions. It also means establishing a higher confidence in an identity based on informed insight.

Dynamic, Adaptive, and Intelligence-driven: RSA Fraud and Risk Intelligence Solutions

With its long history in fraud defense, the RSA family of Fraud and Risk Intelligence solutions counters the evolution of fraud with a comprehensive set of capabilities that herald a growing trend of intelligence integrated with tactics for confronting the fraud industry.

Testifying to these capabilities are RSA's accomplishments in defeating fraud. According to the RSA Anti-Fraud Command Center, RSA shut down more than one million cyberattacks across 185 countries and continues to have an impact worldwide. As this capability grew in response to the growth of fraud as an industry, it led to the development of a coordinated set of capabilities required to counteract well-organized threats to valuable assets.

At the Core: Intelligence and Expertise

Maintaining an effective strategy against modern fraud requires more than a deployment of technologies or implementation of best practices *within* an individual business. Confronting a crime-based industry requires capabilities that counteract fraud at its source. In addition, when incidents occur, specialized expertise in fraud analysis may be required for the proper forensic response. This highlights the role of services that unite expertise and intelligence with action, further extending the concept of layered security beyond narrowly focused protections.

RSA's anti-fraud strengths are centered on a foundation of intelligence with insight throughout the fraud landscape.

RSA's anti-fraud strengths are centered on a foundation of intelligence with insight throughout the fraud landscape. This intelligence is collected and delivered to customers through shared capabilities of their solutions, such as:

- **RSA FraudAction Services,** which provide 24x7 detection, alerting, shutdown, and reporting on fraud activity, also provide a foundation that effective fraud countermeasures can then build on, strengthening defenses against industrialized fraud. Supported by more than 150 analysts at the RSA Anti-fraud Command Center, these services help organizations protect their customers against phishing, malware, rogue mobile apps, and other threats. Clients are provided with details of each attack in order to help mount an appropriate response to future incidents, as well as credential recovery when appropriate.
- The **RSA FraudAction Cyber Intelligence Service** provides detailed analysis on the activities of the cybercriminal underground from not only the normal web, but also the Dark Net, combining intelligence gained from forums with Internet threat trends and organization-specific information. RSA's researchers often directly engage with cybercriminals to uncover specific methods of operation and reveal emerging attack tactics. The RSA FraudAction Cyber Intelligence Service delivers key information around emerging fraud threats including exploit identification, and uncovering unauthorized and fraudulent/mule accounts, underground stores, and emerging fraud infrastructure.

- The **RSA eFraudNetwork** maintains a continuously updated repository of known fraud resources gleaned from RSA's network of customers, service providers, and third party sources worldwide. The telemetry informs RSA's solutions to sharpen their ability to recognize fraud and defeat it before it has a damaging impact. The RSA eFraudNetwork tracks IP addresses, device identifiers, mule accounts, high-risk merchants, and other data in a shared repository accessible to customers to keep them alerted to current trends in fraud activity. This information enables customers to better recognize fraud early and intervene more effectively to protect valuable assets from abuse. Today, one in five confirmed fraud transactions are identified by the eFraudNetwork at the time of transaction.

Integrating Real-time Intelligence With Anti-fraud Technologies

RSA's fraud intelligence capabilities do more than inform customers of fraud activity. Today's anti-fraud technologies also integrate intelligence directly into detection to create real-time defense.

- **RSA Adaptive Authentication** and **Adaptive Authentication for eCommerce Solutions** deliver policy-based protections from fraud specializing in account takeover and misuse. They leverage risk-based scoring features that analyze over 100 risk indicators within the RSA Risk Engine, combined with administrator-defined policies to identify fraudulent activity. Simultaneously, the administrator-defined policies and RSA best practices within the system influence the risk decisions that affect how a user is authenticated. If an activity is above the risk level established by the organization, the system can request additional authentication from the user in the form of challenge questions, an out-of-band SMS code or phone call, biometrics, or any other authentication methods defined by the organization that can be integrated via RSA's multi-credential framework.
- The **RSA Risk Engine** uses the administrator-defined policies and RSA best practices engineered into the system to analyze activities for evidence of potentially fraudulent or malicious behavior scoring the activity in real-time. The Risk Engine collects and analyzes large amounts of data from multiple sources, both internal and external, to the client. It evaluates the online activity using more than 100 indicators of actual or potential fraud and assigns a unique risk score between 0 and 1,000 to each activity. Factors include user behavior, authentication and transaction activity, device identification/characteristics (fingerprint), request context, and more. It employs both a self-learning and adaptive statistical model to maintain currency and accuracy of the assessment. When the best practices within the risk engine are combined with the administrator-defined risk management criteria, the RSA Risk Engine provides an automated assessment of the integrity of observed interactions from login to transaction. RSA's Risk Engine achieves a 91-92% fraud detection rate at a 3% user challenge rate.

  These capabilities are directly consumed in RSA anti-fraud and authentication technologies to manage online activity, dynamically protect access to reduce risk, identify new fraud trends, and defend against them in real-time as they develop.
- **RSA Web Threat Detection** complements RSA's family of fraud-aware consumer identity protection technologies with dynamic insight into malicious activity. Where the RSA Risk Engine is central to Adaptive Authentication, Web Threat Detection gathers session data across Web and mobile sessions from first contact with a remote device. The system analyzes clickstream elements along with custom threat scores and imported data files, such as RSA FraudAction intelligence feeds, to fine tune out-of-the-box rules or configure new ones. Web Threat Detection rules can be created and deployed in seconds and applied to any page on a site subject to fraud or malicious abuse – not just transaction and login pages.

Pre-Access Protections

Before any entity can be trusted with valuable assets, its identity and authorization must be verified. Criminals often seek to exploit weaknesses in account provisioning and proving identity in existing accounts in order to masquerade as legitimate parties or to gain unauthorized access to assets. It is thus an important first step, before establishing *any* relationship between individuals or organizations and their assets, to assure high confidence in the identity of any entity that is being granted access to any asset. This assurance depends on making an intelligence-based verification of identity claimants.

> **It is thus an important first step, before establishing *any* relationship between individuals or organizations and their assets, to assure high confidence in the identity of any entity that is being granted access to any asset.**

- **RSA Web Threat Detection** complements the process of identity assurance pre-login through the collection of forensic data gathered on devices and users from their interactions with customer-facing websites and business applications. RSA Web Threat Detection monitors each click and all HTTP/HTTPS data for every active web session on a site, for comprehensive session intelligence and context in real-time. RSA Web Threat Detection also offers an out-of-the-box rules library with alerts and responses that can be customized and expanded. Rules address high impact areas including application security, account takeover, password guessing and robotic activity that lead to account takeover, chargebacks, and other losses.

  Because website interactions and usage patterns may vary according to a number of factors, this capability is dynamic, adapting the recognition of normal activity as that activity itself changes. For example, site traffic may grow and change in response to seasonal variation, new marketing programs, and changes in website design, sales promotions, or increased referrals from sites such as news outlets in response to a current event. RSA Web Threat Detection recognizes these changes in "normal" behavior as they happen, adapting its analytics to better refine the recognition of threats that stand out and minimize the false positives that could arise in static approaches.

During-Authentication Protections

Once identity is established, protection depends on assuring that fraudulent attempts to access valuable assets are prevented while legitimate access by those authorized is not impacted. As attackers have increased their ability to capture login credentials and exploit many common authentication techniques, organizations must consider the ways in which today's fraud countermeasures can better defend against authentication exploits.

- **RSA Adaptive Authentication** responds to these concerns with a dynamic approach that measures fraud risk at both the time of the authentication and transaction request, and it adjusts the rigor of authentication according to its findings. Its risk-based authentication technology is informed by the RSA eFraudNetwork and powered by the RSA Risk Engine. Currently in use by more than 8,000 organizations in multiple industries, RSA Adaptive Authentication supports strong, multi-factor authentication using a combination of forensic data regarding the endpoint device and behavioral analysis in addition to the intelligence of the RSA eFraudNetwork.

  RSA Adaptive Authentication often functions transparently to users, minimizing the friction users often experience when adopting stronger authentication techniques, thus preserving customer convenience while enhancing confidence in defense. In most implementations, less than 5% of users are challenged. The RSA Policy Manager enables organizations to customize authentication policies to meet their specific needs. Together, a dynamic, intelligence-driven approach (combined with granular control over policy definition) provides organizations with a high degree of flexibility in advanced authentication technology.

RSA Adaptive Authentication protects websites, portals, SSL VPNs, and web access management applications. In addition, **RSA Adaptive Authentication for eCommerce** offers a single fraud prevention solution for card issuers with support for the 3D Secure protocol, and a wide range of authentication and card security products including Verified by Visa®, MasterCard SecureCode™, and JCB J/Secure™.

- **RSA Web Threat Detection** further complements these capabilities by capturing all elements in the clickstream including header details, POST arguments, cookies, geo location, and custom extracted variables. This click-level visibility allows organizations to see how bad actors are navigating on their site, even before a fraudulent transaction is attempted or passed to an authentication solution for additional context and smarter decision making.

Post-Authentication Protections

Strengthening authentication alone, however, will not always defend assets against fraud. For example, consider the class of attacks known as "man-in-the-browser" that echo earlier "man-in-the-middle" tactics of intercepting communications for eavesdropping, picking up sensitive information, and other nefarious purposes – except that "man-in-the-browser" attacks can do all this on a compromised personal endpoint system alone. When a criminal has direct access to an individual's sensitive communications, a high level of visibility into transaction anomalies is required to distinguish legitimate activity from fraud.

This, too, is in keeping with the FFIEC guidance to adopt a layered approach to security. When intelligence includes visibility into transactions, it helps to eliminate what may otherwise be a blind spot in fraud prevention.

- **RSA Adaptive Authentication** combines risk-based analysis of transactional behavior with out-of-band authentication techniques. This layered approach enables organizations to increase the level of authentication needed when fraud risk is detected. Multiple transaction types can be protected, from bill payments to address changes to password resets. When RSA Adaptive Authentication suspects a human or malware threat is creating a fraudulent transaction to a "mule" account, out-of-band authentication with specific transaction verification through out-of-band methods including SMS, phone call, biometrics, or transaction signing via a mobile app can be dispatched to thwart the attempt and prevent damage.

When intelligence includes visibility into transactions, it helps to eliminate what may otherwise be a blind spot in fraud prevention.

RSA Web Threat Detection complements RSA Adaptive Authentication with a robust rules engine capable of examining clickstream elements to generate custom real-time alerts and responses when suspicious activity is identified. This also allows an organization to tailor their response to various types of fraud being perpetrated. For example, response to potential fraud generated by a bot may be different than that of an individual. Features of the RSA Web Threat Detection rules engine include:

- **One-Click Rules** supporting deployment across all pages of a website without having to code pages individually
- **Rule Tags** for identifying rule owners, functional group membership, threat type, and other criteria to enhance reporting capabilities
- **Automated Alert Generation** for the immediate transmission of real-time notification to firewalls, Security Information and Event Management (SIEM) systems, and authentication tools as well as fraud and information security analysts
- **Context Sensitive Rules** allow for the engine to perform actions based on parameters within the rules like designating that a particular action, create a case, or that activities occurring within or outside a particular time period have a higher risk rating

Together, these capabilities highlight how a comprehensive approach creates layered security as envisioned by security standards groups such as that of the FFIEC:

- Gathering of intelligence and expertise
- Applying expertise directly to defense technologies
- Removing fraudulent identity provisioning
- Leveraging adaptive authentication to deny fraudulent transactions *before* they are initiated
- Protecting user transactions once access is gained
- Using comprehensive defenses that employ intelligence and expertise to combat industrialized fraud

EMA Perspective

In technologies such as Dark Net visibility, risk-based authentication, web behavior analytics, and the automation of risk analysis in anti-fraud techniques, RSA's intelligence-driven approach to fraud abatement signals a turning point for combating fraud as an industry. Criminals continually challenge the effectiveness of legacy defenses; insight into malicious activity is becoming central to any effective approach to security and fraud defense. The injection of intelligence directly into defense technologies accelerates the application of countermeasures, enabling organizations to not only detect a wider range of fraud threats, but also stop those threats earlier in the fraud process. To do this effectively, identity and authorization systems are highly dependent on dynamic data sources to sharpen their effectiveness in real-time.

Criminals continually challenge the effectiveness of legacy defenses; insight into malicious activity is becoming central to any effective approach to security and fraud defense.

RSA's fraud defense solutions and services have demonstrated both thought and execution leadership. RSA was among the first companies to validate the value of integrating techniques such as risk-based authentication, device fingerprinting, and user/entity behavioral analysis with web threat intelligence to recognize and stop fraud at each phase of the transaction, with emphasis on stopping fraud *before* it is successful. RSA's anti-fraud approach embodies the adage, "an ounce of prevention is worth a pound of cure."

With its expanding investment in intelligence-driven technologies for identity protection and fraud defense, RSA has become a recognized leader in this field. Its portfolio of products and services embraces a comprehensive approach to fraud defense by exemplifying the concepts of layered security that have become the mandate for any organization that relies on the integrity of its Web or mobile presence, and a pattern for more effective defense beyond.

With a comprehensive approach to fraud and risk intelligence that extends across multiple areas of fraud defense, RSA embraced the scope of the anti-fraud challenge, equipping organizations with the level of response needed to extend the application of layered security to confront what has become an industrialized threat.

With a comprehensive approach to fraud and risk intelligence that extends across multiple areas of fraud defense, RSA embraced the scope of the anti-fraud challenge.

About RSA

RSA, a Dell Technologies business, helps more than 30,000 customers around the world take command of their security posture by partnering to build and implement business-driven security strategies. With RSA's award-winning cybersecurity solutions, organizations can effectively detect and respond to advanced attacks, manage user identities and access, and reduce business risk, fraud, and cybercrime. For more information, go to www.rsa.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3454.100516