RSA® FRAUDACTION™ ANTI-PHISHING SERVICE

End-to-end protection against phishing threats

AT-A-GLANCE

- Gain end-to-end protection against phishing threats from detection to site shut-down
- Prevent new user infections through a comprehensive blocking network
- Track fraudulent activity and lower risk exposure by deploying countermeasures
- Receive actionable data including recovered credit cards and credentials
- Stay updated with information on the latest online threats including new and emerging fraud trends

> "Undoubtedly, the fact that we can rely upon the FraudAction service to keep the uptime of fraudulent sites targeting us to an absolute minimum has helped us to successfully limit the impact that phishing has had upon our institution."
>
> BRIAN O'NEILL HEAD OF TECHNOLOGY RISK & SECURITY NATIONAL AUSTRALIA GROUP EUROPE

The online channel has never experienced such a sophisticated and globally-integrated technological crime network as the one it faces today. Cybercriminals have new tools at their disposal and are becoming more adaptive than ever. Phishing continues to be one of the fastest growing types of online fraud; each month, there are tens of thousands of unique phishing attacks targeting organizations of all types and sizes. And while financial institutions have traditionally been the primary focus, fraudsters are now waging attacks in other industries such as government, healthcare, retail, insurance, and education .

The RSA® FraudAction™ service is proven solution that stops and prevents phishing, pharming and Trojan attacks that occur in the online channel. Offered as a managed service, it enables organizations to minimize resource investment while deploying a solution quickly. It is supported by the RSA Online Threats Managed Services organization, a team of experienced analysts dedicated to staying abreast of the latest trends in online fraud and providing customers with the most up-to-date information.

The RSA FraudAction Anti-phishing service, a core part of the FraudAction service, stops and prevents phishing attacks that occur in the online channel. The FraudAction Anti-phishing service is designed to help organizations prepare for an attack before it occurs, respond to an attack when it takes place, and perform detailed forensics following an attack. And with attacks being hosted from all over the world, FraudAction Anti-phishing technology delivers an integrated network of partners dedicated to providing protection against online fraud originating across the globe.

End-to-End Protection Against Phishing

Phishing still remains a growing threat to organizations across the globe. Not only have the number of attacks continued to increase year over year, but the sophistication level of fraudsters continues to grow, as well. In providing comprehensive, global coverage to our customers, RSA employs a number of measures to ensure end-to-end protection against the threat of phishing including:

- Monitoring and detection
- Real-time alerts and reporting
- RSA Global FraudAction Blocking Network
- Site shut-down
- Forensics and credentials recovery
- Countermeasures – baits operations

The RSA Anti-Fraud Command Center

At the core of the FraudAction service is the RSA exclusive Anti-Fraud Command Center (AFCC). An experienced team of fraud analysts, work 24x7 to shut down fraudulent sites, deploy countermeasures and conduct extensive forensic work to catch fraudsters and prevent future attacks. The AFCC has established direct, open channels with thousands of hosting authorities around the world, including ISPs, domain registrars, and web hosting services, and provides multi-lingual translation support in nearly 150 languages to further enhance its ability to detect, block and shut down fraudulent sites.

The AFCC is leading the way through results. RSA fraud analysts:

- Have shut down more than 500,000 phishing attacks – the highest shutdown volume for any single provider in the industry
- Work with more than 14,000 different hosting authorities scattered around the globe
- Maintain one of the best shutdown medians in the industry. FraudAction's shutdown median for US-hosted attacks is just 5 hours, and just 6 hours for attacks hosted worldwide.
- Serve over 450 FraudAction customers, including many Fortune 50, 100, and 500 companies.

- **Monitoring and Detection.** FraudAction's multiple detection sources enable RSA to scan over 30 million URLs per day, and perform both automated heuristic and manual qualification of suspicious URLs. To maximize the early detection of phishing attacks and prevent fraud from occurring at all, multiple early detection strategies are employed, including the monitoring of customers' weblogs and abuse mailboxes, and ongoing research of known rogue servers. Providing high quality detection feeds, RSA detection partners include top notch ISPs and email security companies, such as Commtouch, AOL, and Yahoo.
- **Real-time alerts and reporting.** Once a suspicious URL is confirmed to be a threat, customers are immediately notified. The FraudAction Anti-phishing service also includes a user-friendly web-based dashboard tool that is updated in real-time with the latest threat information.
- **Exclusive site blocking network.** The RSA Global FraudAction Network helps provide a first line of defense to 90% of the world's web traffic. In addition to users of Internet Explorer, Chrome, Firefox and Safari, RSA's blocking feed also benefits customers of leading data security providers and ISPs, such as McAfee, Commtouch, AOL, Yahoo, Checkpoint, and Radware. Our strategic blocking partnerships ensure that hundreds of millions of online users are prevented from accessing confirmed phishing and malware sites, even if they click on a link within a phishing e-mail.
- **Site shut-down.** The AFCC leverages its strong, long-standing relationships with over 13,800 different hosting authorities and its multi-lingual capabilities to enable the quick shut down of fraudulent sites on a global scale. To date, the AFCC has been responsible for performing the targeted shutdown of offending IP addresses and domains used to launch over 500,000 attacks in more than 185 countries.
- **Forensics and credential recovery.** AFCC fraud analysts conduct a forensic investigation of each attack in an attempt to extract additional valuable information, such as the phishing kit used to launch the attack, victims' compromised accounts, and fraudsters' e-mail drop accounts. FraudAction Anti-phishing customers also receive a feed of compromised payment card accounts, allowing them to block accounts before they are used to commit fraud.
- **Countermeasures.** RSA offers customers various countermeasures, such as baits operations, which enable financial institutions to identify phishers' cashout schemes and methods of operation. Baits operations consist of feeding specially-designed login credentials into a phishing attack, and tracing any ensuing fraudulent activity perpetrated with those same credentials. Follow up analysis of a baits operation enables customers to take corrective measures, such as updating security systems and authentication procedures.

Optional Feature: Anti-Pharming

The RSA FraudAction service also offers an optional anti-pharming feature. The RSA FraudAction Anti-pharming service actively monitors the Internet for poisoned DNS servers and upon identification and/or confirmation of a suspicious match; customers are immediately notified of the threat. The AFCC will then work on shutting down the fraudulent site as well as contacting the owner of the poisoned DNS in order to correct the issue.