The RSA eFraudNetwork
Global repository of fraud data increases detection

The RSA eFraudNetwork can help organizations proactively identify IP addresses, mule accounts, devices (including mobile), merchants, and other indicators and patterns that have been involved in fraud (or a fraud attempt) across more than 150 countries. The RSA eFraudNetwork is the industry’s first and largest cross-institutional, cross-platform, international shared online fraud network. In existence for multiple years, it has thousands of contributors worldwide, including financial institutions, credit and debit card issuers, healthcare firms, telecommunications companies, retailers, internet service providers, wireless providers, high-tech companies, government, and law enforcement agencies.

Shared fraud intelligence can prevent losses from occurring by enabling organizations to proactively combat known cybercriminals. RSA monitors and tracks fraud and fraud attempts across an extensive network of customers, ISPs, and third-party contributors. When fraud is confirmed by one of the organizations, the different elements (such as IP, hashed International Bank Account Number [IBAN], device elements and more) of the fraudulent transaction are shared in the eFraudNetwork. Much more than an IP blacklist, the fraud intelligence information in the eFraudNetwork is continually updated by eFraudNetwork contributing partners, RSA Fraud and Risk Intelligence customers, as well as analysts at the RSA Anti-Fraud Command Center (AFCC).

The intelligence in the eFraudNetwork not only comes from multiple sources but also includes many different types of data elements, such as IP addresses, device fingerprints, cookies, mule accounts, mobile device identifiers and more. These elements are continuously identified, evaluated and scored according to their up-to-date risk level to ensure that the information in the eFraudNetwork is timely and accurate.

The eFraudNetwork algorithms dynamically set expiration dates and risk scores for all of these data elements based on case management feedback on confirmed (and false) fraud, a unique authentication feedback loop and frequency. This intelligent scoring method based on fraud-to-genuine ratio and frequency using machine-learning algorithms increases the effectiveness of the eFraudNetwork.

The eFraudNetwork is a reliable data source—no personally identifiable information is shared and all data is cleansed prior to being added to the repository.

A Case Study with a Global Financial Institution Showed:

- Over $2.5M fraud savings a quarter were a result of eFraudNetwork alone*
- The eFraudNetwork had a low 0.4% false-positive rate.**
- There was only a 0.12% intervention rate (challenged or declined transactions).

* Fraudulent transactions that included an element that was in the eFraudNetwork
** Transactions that included an element from the eFraudNetwork but were eventually marked as “confirmed genuine”
eFraudNetwork in numbers

- Thousands of direct and indirect customers are contributing to RSA eFraudNetwork confirmed fraud intelligence daily.

- Fraudulent elements from 11 million confirmed fraudulent transactions are contributed daily.

- Around 350,000 elements to the daily feed, showing the significant correlation of fraudulent transactions across customers (as the same fraudulent elements are present in transactions coming from different customers, increasing the indication that these are indeed fraud related).

- Over 64 million yearly transactions include elements that were shared in the eFraudNetwork.

- RSA eFraudNetwork saved $365 million a year for the RSA Fraud & Risk Intelligence customer base.

- RSA Adaptive Authentication for eCommerce customers enjoy an average false-positive ratio of only 0.87% (transactions that included elements from eFraudNetwork but were marked as “Confirmed Genuine”).

“Partnering in the RSA eFraudNetwork service has accelerated our learning about anti-fraud technology and developing a comprehensive fraud strategy. In fact, it’s been such a success that what started out as a single project has now extended into other areas of the bank and will be developed even further.”

—Fraud Strategy Manager
The power of collective fraud intelligence

The power of the eFraudNetwork ecosystem is rooted in its ability to capture data elements for fraud that have already occurred, and then making that intelligence available across the network.

RSA Fraud and Risk Intelligence customers can be automatically enrolled in the eFraudNetwork. Direct feeds of real-time fraud threats are leveraged by the RSA Risk Engine, which powers RSA Adaptive Authentication, RSA Adaptive Authentication for eCommerce and RSA Transaction Monitoring. When a transaction or an activity is attempted by a device, IP address or other element that appears in the eFraudNetwork as fraudulent, it will impact the overall risk score. In addition, eFraudNetwork elements can be referenced directly in the Policy Manager of the respective solutions.

Connected, shared information provides better security than siloed, disconnected environments. The RSA eFraudNetwork allows customers to benefit from the cumulative fraud intelligence gleaned from a community of thousands of organizations across the globe.
About RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.