Addressing the Big 3: Compliance, Fraud & Cyber Security

When investing in new security technologies, credit unions should look for solutions that intersect as many of these three items as possible. They should look for solution "overlaps" where an implementation will help them with compliance issues while simultaneously helping them with cyber security, for example. The problem is that regulations all too often trail the fraudsters' actions simply because they are so creative and increasingly sophisticated in their methods. Existing policies and procedures are inadequate. A credit union could pass an internal audit or external examination, yet still be successfully attacked – being compliant is just the starting point.

Attacks against smaller financial institutions are increasing in number, duration, and complexity. In order to effectively address these attacks and protect their member's PII and finances, credit unions need to put an end to end fraud mitigation solution in place. A multi-layer defense takes into account the three phases that criminals employ: 1) attack setup; 2) attack launch; and 3) the actual movement of the data or funds. Unfortunately, these stages can be spread out over long periods of time and over different channels such as online, contact center, branch, mobile, etc. At Easy Solutions, we offer protection at all three stages to ensure that your systems are secure. We help credit unions implement a flexible and comprehensive multi-layered defense across all devices, channels and clouds.

When you have visibility across all of your channels, it makes it much easier to detect fraudulent activities from both outsiders and employees. Transaction anomaly detection is a critical component of this visibility and is a great tool for delivering real-time threat intelligence. It helps stop fraud even after criminals have compromised every other security layer meant to protect your members. Our highly customizable Suspicious Activity Analyzers detect transaction patterns linked to money laundering, cloning and other nefarious activities.

In terms of cyber-security, the explosion of the mobile banking channel, driven by the widespread adoption of smartphones and tablets as well as shifts in consumer behavior, is both a huge opportunity and a potentially unbounded risk. As with the emergence of online banking over a decade ago, no long history of channel-specific fraud exists in order to help tune anti-fraud and security investments. Credit unions should expect that the threat landscape facing the mobile channel should follow (in a general sense) the trajectory of online threats, but at a faster pace. Credit unions should not expect highly prescriptive guidance from regulators and we should expect regulations to follow the threat, not precede it.

Credit unions should focus on "surrounding" the mobile and online threat with a combination of controls. This can be achieved by real-time monitoring of the digital threat environment, understanding more about the health and security of the consumer devices connecting to mobile and online banking to limit account takeovers and to limit the usefulness of compromised accounts by implementing MFA and transaction monitoring. This layered approach recommended by FFIEC and NCUA is highly pragmatic, scalable, flexible and effective. At Easy Solutions, we completely enable this approach because our Total Fraud Protection® Strategy offers a multi-Layer portfolio that addresses all of these different stages in the life cycle of an electronic attack allowing us to prevent fraud in a truly proactive way.

Daniel Ingevaldson
Chief Technology Officer

EASYSOLUTIONS

Daniel Ingevaldson is Easy Solutions' Chief Technology Officer. With over 15 years of experience protecting some of the world's biggest organizations from next-generation threats, Daniel is our guru when it comes to developing fresh approaches to online security and fraud. As our CTO, he defines and executes the strategies for researching and creating the next phase of Total Fraud Protection®products. Daniel was co-founder of Endgame Systems, Inc., a start-up focused on building advanced network security technology for United States government clients.

Contact Info

www.easysol.net