DEFENSESTORM
THE BEST OFFENSE.

GRID Active Fraud Prevention

GRID Active Fraud Prevention provides continuous monitoring and alerts from data across the network, online banking platform and CORE to proactively prevent cyber fraud

Built For Banking

Financial institutions (FIs) have too much at stake – financial loss, reputational damage, business continuity – to tackle these challenges alone when it comes to managing cyber risk. We recognize the unique risks that FIs encounter when it comes to cyber crime. Therefore, we developed a customized solution to address those distinct cyber risk challenges to provide optimal protection for banking.

Proactive Approach to Cyber Fraud

Although many FIs rely on BSA/AML providers to detect fraud (SAR/CTR filing to FinCen, OFAC/314b Screening, Know Your Customer Standards), proactive fraud prevention is not their primary focus. These fraud detection solutions provide batch or next day alerting, have limited rule configuration and only focus on transactions, which leaves the FI the task of recovering lost funds after they have left the institution.

Account Holder Fraud Prevention is uniquely positioned by providing a proactive approach to stop fraud before funds ever leave your financial institution. The solution provides active threat detection that correlates information from your network, online banking platform, core, and the dark web providing real-time alerts and intervention. Proactively stop fraud related to scams, account takeover, online account opening and insider threats to better protect your institution, your bottom line, your reputation and, of course, your customers and members.

Every $1.00 of fraud loss now costs U.S. financial services firms $4.41

Source: 2023 edition of the LexisNexis® True Cost of Fraud™ Study

GRID Active Fraud Prevention

FEATURES

- **Real-time alerting**
- **Non-monetary account update alerts**
- **All required enterprise-wide Integrations**
- **On-the-fly rule creation and editing**
- **Community watch lists and information sharing**
- **Evidence gathering /case management**

BENEFITS

- **Fraud Prevention fully integrated with cybersecurity, governance and risk assessment**
- **Proactive fraud prevention before any loss occurs**
- **Enable Fraud Fusion Center capabilities**

Another avenue FIs may choose is to deploy point fraud products that only cover one specific area cyber criminals use to initiate fraud. This approach creates a complex landscape of point solutions that is difficult to manage and can leave FIs open to vulnerabilities since fraudsters are often able to bypass the solutions/products.

DEFENSESTORM
THE BEST OFFENSE.

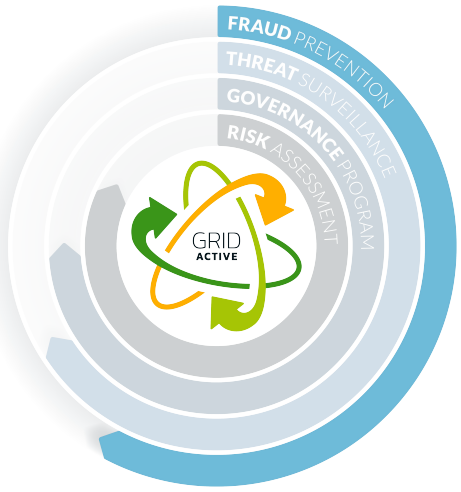
GRID Active Fraud Prevention

Proactive monitoring and prevention against cyber fraud

Account Holder Fraud Prevention is a part of an overall cyber risk management platform, built on and integrated our intelligent data engine, GRID Active, that constantly gathers, analyzes and reports real-time insights on evolving cyber risk and integrates cyber risk software products, technology and capabilities.

Proactive Fraud Prevention with Consolidated Evidence Collection

- Correlation of non-monetary and monetary activities to prevent fraud before it happens to save FI time, resources, brand reputation
- Real-time alerts so FIs can block suspicious activity, execute step-up authentication, and route anomalies to analysts for further investigation to ensure threats are seen early.



Multi-Channel Fraud Protection with At-A-Glance Visualization of Fraud Threats

- Ability to monitor, detect, and alert on suspicious activity across all departments – including Originations, Online and Mobile banking, and Internal Fraud – for an integrated approach to managing risk across the organization.
- Proactively defend against fraud attempts across channels including:
    - Fraudulent account opening/loan applications by detecting if multiple submissions have come from the same IP address, phone, or email.
    - Account takeover attempts through recognition of multiple concurrent account logins from different locations.
    - Employee Activity Monitoring to detect if employee actions and permissions fall outside of their role or FI policy.

Comprehensive Threat Visibility through Integration with cybersecurity and risk processes

- Correlating cybersecurity data on the network with online banking events, banking core activity, dark web intelligence, and a consortium of threat sources for one consolidated view of threats.
- Bridge the gap between Info Sec and Fraud teams for a more cohesive approach to preventing fraud and managing risk.
- On the fly rule creation and deployment that enables your fraud and a cybersecurity team to respond to an emerging attack in real-time.