

Identify Scam Vulnerabilities With IFM

Some customers fall prey to fraudulent scams at a higher rate. They remain a significant challenge for financial institutions, like yours, because it's difficult to proactively identify them.

Recent guidance and legislation encourage firms to identify and track customers likely to fall victim to scams across all their products and services and give each customer an appropriate level of care given their characteristics.

With IFM, you can proactively identify customers at risk, enabling your organization to put the right controls in place to significantly reduce successful scams, but only where appropriate. Protect your firm and safeguard your customers.

How IFM Identifies Customers Vulnerable to Scams

All customers are at risk of falling for a scam, but to differing degrees. IFM assesses each party holistically to give them a scam vulnerability score.

The scam vulnerability score factors in four categories of characteristics that increase the likelihood of a customer becoming vulnerable to scams:



Life Events: A big, life-changing situation—either planned or unexpected—that can impact a customer, such as getting a divorce, losing a job, or retiring.

IFM assesses all life events, both positive and negative, as well as supporting attributes like number of dependents, subpoenas, and citizenship status. Negative life events in particular hinder customers' ability to make sound decisions and represent their own interests.



Resilience: Low ability to withstand financial or emotional shock. The lack of resilience can directly impact a customer's ability to recover from a negative life event.



Capability: Low knowledge of financial matters, low confidence in managing money, and low capability in other relevant areas such as literacy or digital skills. Undeveloped or underdeveloped skills limit a customer's means to overcome life events, for example find a new job.



Behavior: A customer's transactional behavior. Evaluating if a customer's behavior deviates from their normal pattern allows financial institutions to identify situations involving social engineering.



NICE Actimize research indicates that customers who were victims of a fraud attack are more likely to be scammed in the future. IFM also collects information about past scams and fraud attempts on the customer's accounts to improve the predictive-nature of the scam vulnerability score.

How a Scam Vulnerability Score Improves Anti-Fraud Programs

By combining the scams vulnerability score with existing detection, you can deploy a layered defense. Your firm can use the scam vulnerability score to effectively spot customers who are likely to be scammed that traditional transaction-based and typology-based models wouldn't have picked up. The score and relevant information can also be used as an input to strengthen your own scams monitoring models.

Your fraud strategists can incorporate score and risk insights into their fraud strategy rules. For example, fraud strategists can implement a targeted approval process for risky transactions for a specific subset of customers while ensuring that other customers experience a lower level of friction.

With the scams vulnerability score, you can use entity-centric insights to improve all of your data-driven fraud processes.

Protect Customers from Scams and APP fraud with IFM's Scams Vulnerability Score.

→ [Schedule a demo](#)