PAY before
prepaid.mobile.emerging payments.

Viewpoint

In Viewpoints, prepaid and emerging payment professionals share their perspectives on the industry. Paybefore endeavors to present many points of view to offer readers new insights and information. The opinions expressed in Viewpoints are not necessarily those of Paybefore.

No. 1 Fraud-Fighting Strategy: Self Examination

By Daniel W. Draz, Fraud Solutions

It's safe to say that the only real constant about fraud is change. In fact, fraud is so dynamic and fluid that fraudsters constantly are adapting their techniques to fit an industry's services and product offerings. Fraudsters even adapt their strategies to target a particular company. Many companies, however, can't say the same about their corporate anti-fraud efforts, which are largely inactive, stagnant and static. But, keeping up with the fraudsters is absolutely imperative in the "target rich" financial services industry.

The first step is recognizing the changing fraud landscape by shifting from a reactive fraud approach to a highly proactive, robust and holistic fraud program. This is a significant key to getting out in front of the complex fraud problem. To make the change, I recommend a five-step approach:

1. Conduct a thorough evaluation of your entire organizational anti-fraud efforts involving fraud detection, monitoring, analysis, investigation and risk management.

2. Benchmark your team's performance against industry anti-fraud standards (i.e., best practices).

3. Determine and confirm the root cause of existing performance issues.

4. Assess anti-fraud policies, practices and procedures addressing critical deficiencies.

5. Implement forward-thinking, targeted solutions that meet the increased needs of a fraud unit in the financial services sector.

The goal during this exercise is to increase your staff's overall performance and fraud-fighting effectiveness; increase analytic, trending, metric and technical capabilities; increase individual employee awareness about prepaid fraud trends; and decrease the fraudster's abilities to easily commit fraud against your customers, products and services. The three major assessment components when performing a fraud unit performance and gap-analysis evaluation of this nature revolve around people, processes and technology.

People

While having ample staff to do the job is certainly an important part of the process, the answer isn't always hiring more employees. Staffing is a critical part of the evaluation, as an under-

Daniel W. Draz, M.S.,CFE *is the principal of Fraud Solutions, a global fraud consulting firm located outside Chicago. Draz is a recognized leader in the fraud profession, providing innovative anti-fraud strategies, insightful observations, fraud training and thought leadership to clients. He works with companies, including those in prepaid and emerging payments, on their fraud risk management efforts. He can be reached at dan@fraudsolutions.com.*

No. 1 Fraud-Fighting Strategy: Self Examination

staffed team certainly may be a factor, depending on the volume of business conducted, referrals generated to the team and SLA expectations.

Historically speaking, we know that some companies, even when staffed properly, have ineffective fraud units and root-cause analysis leads to other contributing factors like management philosophies; insufficient management support; ineffective or outdated policies, processes and procedures; inadequate technology platforms and lack of staff training.

When evaluating underperforming fraud units, it's imperative to ensure that employees' skill sets are equally matched and balanced to the anti-fraud tasks assigned to them. It's not uncommon to find employees struggling in fraud positions only to discover a mismatch between the tasks assigned and tools available to detect, investigate, analyze and mitigate potential issues. Further examination also may reveal that faulty anti-fraud policies, processes, procedures and training are the underlying culprits.

Faced with a number of complex business and anti-fraud issues, and the changing face of global fraud, it's often difficult to isolate the performance of an underperforming fraud unit to only one of the core assessment elements. It's entirely possible that performance issues actually are a combination of the people, processes and technology not functioning effectively.

Lastly, given the changing fraud trends it's critical not to overlook your annual employee training and continuing education programs to ensure they're relevant, timely and topical. Regular training is required to ensure a professional knowledge base among the employees on your fraud team and to help them function effectively.

"Ensuring that your team is using state-of-the-art and robust technology platforms to generate and adjudicate alerts, and manage investigations, is a solid first step. However, post purchase is most often where companies drop the ball."

Processes

It's also imperative to critically examine the fraud referral process flow from end to end, identifying operational gaps and opportunities for service improvement. While it's easy for employees to place the blame for operational deficiencies on the volume of transactions, that may not be the performance culprit.

If you don't know where the process hitches are, one easy step is to simply ask your employees. Empowering fraud team employees to participate in the evaluation process is critical to the team-building process and has a twofold effect. First, given an opportunity to solve problems, team members often respond with insightful and innovative solutions because they're vested in the team's success. Second, the opportunity to be part of the solution, and the recognition that management values their opinions, fosters a corresponding increase in individual and team morale, which often reenergizes and refocuses your fraud team.

Armed with the results of your analysis and employee feedback, the next step is to retool the clunky processes and procedures in accordance with the project's goals. Revised processes and procedures, which more closely reflect current fraud trends and activity, ensure a more fluid fraud referral flow from start to finish. In fact, a tweak in one core assessment area oftentimes has a direct and corresponding effect on another area improving process flows, staff performance and efficiency.

Since handling processes and procedures are sub-components of the company's main fraud policy, major process and procedure changes necessitate a change, or update, to the fraud policy as that is the repository of all underlying anti-fraud documentation. In fact, the fraud policy should change over time in direct response to regulatory requirements, the nature of the fraud landscape, the type of business and customer demographics.

Internally, the revised fraud policy should then be disseminated to internal and external company stakeholders, ensuring awareness, compliance and a seamless transition. Improved operational processes and communication are key components in launching a revised anti-fraud effort.

Technology

The technology platform is the backbone of any good anti-fraud operation, but technology alone isn't the answer to efficiency or the fraud-detection problem. It's not uncommon for companies to have an excellent fraud technology platform but an underperforming fraud team because the employees are responsible for acting on the data produced by the technology tool.

In-depth analysis of anti-fraud technology tools often reveals significant performance issues, which may be caused by the functionality of the tool itself, the personnel using the tool or

No. 1 Fraud-Fighting Strategy: Self Examination

how they're using it. Ensuring that your team is using state-of-the-art and robust technology platforms to generate and adjudicate alerts, and manage investigations, is a solid first step. However, post-purchase is most often where companies drop the ball. Thinking technology solves the entire fraud problem, some companies fail to review the analysis processes used to evaluate system output, which is necessary to support the team's business operations more efficiently.

Concerns with any new anti-fraud technology platform are twofold: whether the product closely matches your company's current business demands and, perhaps more importantly, whether it has the bandwidth to expand as your business volume and anti-fraud efforts grow in the years ahead. These criteria are imperative as technology purchasing mistakes are not only costly but often directly impact other business units, such as IT, training, customer service, compliance and legal.

Other Considerations

Comprehensive analysis of a fraud unit's people, processes and technology often identify other issues that require immediate attention:

- **Red flag rules and conditions flagging suspicious or anomalous transactions:** Compare all alerts against results to determine if certain alerts are the result of obsolete or ineffective rules generating a high percentage of false positives. Modify alert criteria as needed to reduce the rate of false positives. This ensures your fraud team is working on the real thing and not spinning its wheels needlessly.
- **Metric, trending and analytic capabilities:** Determine whether the technology platform your company is using has the capability to generate advanced, meaningful and actionable reports. A key to an effective transactional anti-fraud unit is the ability to analyze critical fraud data, assess the trends and implement proactive anti-fraud strategies in a forward-thinking manner before the fraudsters get there. Trending is one of the keys to getting out in front of a fraud pattern proactively, but also helps senior management assess the profitability of a block of business. Many of the companies in the technology area, like Actimize (transactional monitoring) and Column Technologies (investigative case management), offer metric, trending and analytic capabilities at the touch of your fingertip, which provide customizable dashboards for management review.
- **Communication protocols:** Assess the communication processes between the fraud unit and senior management, as that is often a malfunctioning process. Effective communication flows are necessary to address critical incidents in a timely manner, meet regulatory requirements and get real-time approval to modify ineffective processes, procedures or underperforming rules.
- **Law Enforcement Interaction:** In many financial services companies, effective interaction with law enforcement is significantly lacking. Some of my clients have addressed this issue with the creation of enhanced law enforcement and prosecutor outreach efforts, including increased awareness and educational campaigns, regular communication methodologies, and more direct contact with law enforcement agencies handling the types of fraud issues they deal with and cases they may refer. While not all cases get accepted for prosecution consideration, these outreach efforts have been known to generate increased numbers of cases accepted, investigations conducted and successful prosecutions of people suspected of committing fraud, which often serves as a significant deterrent to others who may be thinking about doing the same thing.

Review, Revise, Repeat

There are a number of reasons to conduct a top to bottom fraud unit review referenced in this article. One of the more compelling reasons is that fraud units that operate more efficiently in detecting, investigating, analyzing and preventing fraud increase the company's anti-fraud ROI.

Evaluating your company's anti-fraud efforts regularly is paramount. A retooled, redesigned and reenergized fraud program—utilizing effective new policies, processes, procedures and a cutting-edge, transactional software analytics and investigative case management platform—should be the backbone of your anti-fraud efforts. Doing so, your business will be better positioned to tackle the constantly changing, global fraud challenges in the prepaid industry more effectively than ever before.

However, the consequences for failing to regularly evaluate, manage and update your anti-fraud efforts are significant as criminals always seek out financial services businesses with lax, non-functioning or non-existent anti-fraud protocols or technology. Being seen as the weak link is like a neon "Open" sign for criminals looking for an easy pay day. Perhaps more importantly, however, are financial performance considerations where losses associated with fraud not only show up on regulators' radar screens but detract significantly from your company's reputation, customer base and bottom line.