First Data Market Insight

Eight Tips for Reducing Fraud and Bolstering Data Security

With fraud and data security threats coming in so many different forms and from so many different channels, financial institutions must gain a better understanding of how criminals operate and how risk management is changing. With this understanding, you will have a better chance of mitigating the risks and recognizing attacks before they do serious damage. In addition, financial institutions need to adjust fraud detection and prevention strategies to keep up with the evolving trends. In some cases this means investing in new technologies; in others, it means bridging organizational silos. In all cases, it means improving your odds of detecting a threat before it reaches the customer. With this in mind, here are eight ways to improve data security and reduce fraud:

Maintain Regulatory Compliance

Various federal laws and industry mandates designed to improve information security have been enacted over the past several years. Complying with these regulations—most notably the FACTA Red Flag Rules, Payment Card Industry Data Security Standard (PCI DSS) and Gramm-Leach-Bliley Act—enables institutions to avoid potential regulatory penalties and is a first step towards protecting sensitive cardholder data and reducing fraud. FIs should also keep abreast of pending legislation in order minimize surprises and disruptions associated with future regulations.

Safeguard Customer Data

Ensure that the appropriate controls are in place to protect customer data from external data breaches and employee theft. This should start with a comprehensive risk assessment to identify the information that needs to be protected and to assess potential vulnerabilities. Seek external advice, if necessary, to ensure that your firewall technology and data encryption standards are appropriate and up-to-date. Effective employee screening using background checks and shared negative files can help reduce the threat of internal fraud.

Enlist Your Customers in the Battle

Let customers know what you are doing to prevent and detect fraud and data compromises. Encourage customers to take responsibility, as well. Educate them on emerging fraud threats and steps they should take if they believe fraud has occurred. Include communication to help them understand the benefits of opting-in to paperless statements, reviewing their account activity regularly in order to detect fraudulent activity, learning to spot skimming devices, and securing their computers with up-to-date Internet security software. It is also important to provide guidance to them on the potential hazards of social media and the risks associated with using mobile devices.

Deploy the Latest Fraud Management Technologies

Validating the identity of potential customers is an important first line of defense against account fraud. Consider deploying next-generation identity verification technology (such as First Data's SafeID Verification Score solution) to accurately and efficiently validate potential customers through predictive analytic models and risk scoring. Neural network and predictive software technologies (like those found in First Data's Fraud and Risk Premium Package) represent just a couple of innovative solutions being deployed by institutions to cost-effectively detect and prevent fraud in real-time. Because fraudsters follow the path of least resistance, institutions that lag the rest of the industry in implementing advanced detection solutions make themselves especially vulnerable. And fraud management doesn't end with blocking the authorization: you also need automated back-end tools that allow you to communicate effectively with cardholders to notify them about fraudulent activity, reissue cards, and preserve accountholders' confidence in your institution.

Use a Layered Approach to Managing Risk

Don't rely on any single method for data security and fraud management. For example, in addition to deploying analytics solutions to flag or block potentially fraudulent activity, train employees to spot suspicious transactions, and offer e-mail and text alerts to customers for particular transaction types like wire transfers and foreign purchases. To be proactive about fraud prevention, it's important for financial institutions to understand the fraud that's happening in their own portfolios and keep on top of what is happening in the industry, as well. Be diligent about adding to or updating the layers; this isn't a one-time fix.

Implement an Enterprise-Wide Fraud Management Strategy

Many banks and credit unions continue to manage fraud according to institutional silos, delegating this responsibility to individual business units and product types. Integration of fraud management into a centralized, cross-product function enables institutions to share resources and data, capitalize on economies of scale, and better coordinate tactical approaches—resulting in reduced fraud losses and a more consistent customer experience. A preliminary step toward implementing an enterprise fraud management strategy can be to establish a shared internal database of fraud events and perpetrators. In addition, all financial institution employees should be trained to detect and prevent fraud, both external and internal. Institutions should also have a clear process for reporting suspected fraudulent activity.

Don't Overlook Simple Operational Controls

There are a variety of easy-to-implement operational policies and procedures that can significantly improve data security and reduce the risk of fraud:

- Don't allow customers to use their Social Security number as an online banking username.
- Require additional authentication and positive confirmation for executing accountholder address, phone and e-mail changes.
- Implement regular, systematic checks of ATMs for evidence of skimming devices, hidden cameras and other irregularities.
- Mandate that employee computer passwords be changed at regular intervals.

Be Prepared for the Worst

Careful operations planning and preparation can control costs, improve customer loyalty and preserve your reputation if the unlucky day arrives and your institution is affected by a data breach. Work with a risk management expert in advance to develop an effective response strategy that will mitigate the potentially disastrous effects of a data breach. The proper strategy should include forming a cross-functional event response team, creating a risk assessment and response matrix, and devising a post-event communication plan.