A 360° Degree View Can Lead to Added Security

Identity management has several implications for businesses in almost every industry. This is especially true for organizations offering products and services via online and mobile channels. For these organizations, identity management has become an enabler of core business functions, from improving service delivery and transaction volume to achieving compliance—and mitigating fraud.

Each year, global organizations lose an estimated five percent of revenues, approximately $2.9 trillion, through fraud.[1] Identity theft, whether from criminals dumpster diving to gather a victim's personal information or paying an employee for access to customer account data, is a root cause of fraud.

While methods can evolve, usually in response to new fraud prevention practices, one thing is constant: fraud is committed by individuals. Thus, knowing the parties with whom you do business can help prevent fraud in the first place. To protect your business, it is important to assess your risk from a 360° degree view that includes your customers, your employees and your vendors.

The three elements that lead to fraud, known as the theory of the "fraud triangle," include motive, perceived opportunity and rationalization for monetary gain.[2] Given the proper convergence of these elements, individual customers, employees and vendors—or any combination thereof—can be motivated to commit fraudulent activities.

Knowing your customer extends beyond individuals to include corporate partnerships, charities, trusts and other entities. For customers, both new and existing accounts can pose fraud risks as opportunities can arise throughout the customer lifecycle. It is important to regularly monitor accounts and include online, mobile, automated and other channels as part of ongoing identity management programs.

Ongoing identity management also extends to employees. Criminals will approach employees who appear receptive to payment for providing access to customer data. It is not uncommon for criminals to offer payment exceeding the employee's annual salary or threaten bodily harm to gain cooperation.[3]

Vendors providing outsourced services, such as information technology or marketing, can also perpetrate identity fraud. They might have access to account data that one of their employees can obtain for fraud purposes. Vendor fraud can also include inflated or phony invoices; the vendor works with an employee of the targeted organization who approves the invoice in return for a kickback.

An effective, automated identity management plan using multi-factor authentication can help reduce fraud costs while enhancing business efficiencies, customer satisfaction, compliance and revenue. In addition, sharing data about fraud schemes and identity management technologies can help businesses create proactive fraud prevention strategies—rather than reacting to fraud after it occurs.

To find out how to protect your organization from fraud or learn more about identity management, visit http://idmanagement.lexisnexis.com

LexisNexis®

[1] Association of Certified Fraud Examiners, 2010 ACFE Report to the Nation on Occupational Fraud and Abuse, 2010, <http://www.acfe.com/resources/publications.asp?copy=rttn > and < http://www.acfe.com/rttn/rttn-2010.pdf > (June 2, 2010).

[2] Cressey, D.R. Other People's Money: A Study in the Social Psychology of Embezzlement, Free Press, Glencoe, Illinois, 1953.

[3] Office of the Comptroller of the Currency, OCC Alert 2002-4: Organized Gang and Teller Collusion Schemes, Apr 25, 2002, <http://www.occ.treas.gov/ftp/alert/2002-4.doc> 30 May 2008.