Five Questions for Mitigating Fraud Risk Through Identity Management

Knowing Your Customers is Key to Mitigating Risk and Improving Service

Not knowing enough about your customers poses fraud risks that can lead to significant losses in both revenue and brand reputation. These risks can affect organizations across nearly every industry, whether from the illegitimate receipt of government benefits, fraudulent retail transactions, illegal access to online utility or financial accounts and other fraudulent activity in industries such as healthcare, telecommunications and any company issuing credit.

To help prevent losses arising from the misuse of personal information, organizations should implement an identity management solution to reconcile the identities of new and existing customers. This makes identity theft a high-risk activity with zero reward. The framework for a comprehensive identity management process boils down to five questions:

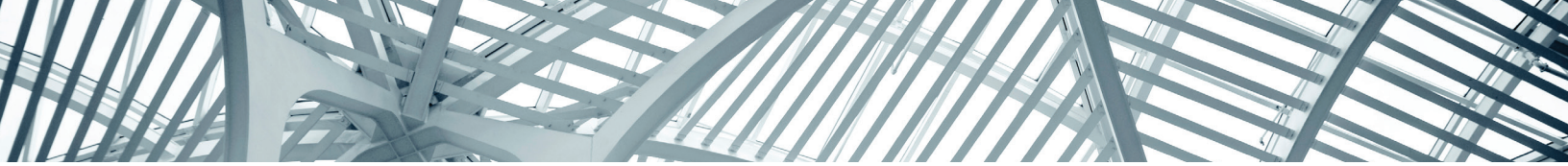
	RESOLVE	VERIFY	AUTHENTICATE	EVALUATE	ALERT
Know Your Customer Tools	Who are you?	Do you exist?	Are you who you say you are?	Can I do business with you?	Are you exhibiting high-risk behavior?

From initial discovery to ongoing alerts, new and existing customer authentication efforts help mitigate fraud risk.

RESOLVE: "Who are you?"

This can be answered by gathering the kind of contact information often requested on a basic application or enrollment form, such as first and last name, current address, and telephone number. Partial information, such as month or year of birth and last four digits of a social security number, can be cross-referenced to determine additional information such as address history or other necessary identifiers.

LexisNexis®



VERIFY: "Do you exist?"

Next, verify the information by checking it against public record databases. This is important because data from various sources might be valid individually but may not all belong to the same person. For instance, criminals often use stolen SSNs or driver's license numbers, or those of deceased individuals, to perpetrate fraud. You can address this by using public record data to match the name to the address or the driver's license number to the name. While it's important to verify that the data is associated with the person in question, it is also necessary to determine if the person is using multiple identities or multiple people are using the identity presented. Any discrepancies are reason to perform further due diligence.

AUTHENTICATE: "Are you who you say you are?"

Confirming that an identity exists does not confirm that it belongs to the individual presenting it. Knowledge-based authentication techniques such as interviews or questioning are most commonly used to help reconcile your customer's identity. For example, you can present the customer with challenge-response questions that ask about random elements of a person's biographical information, such as prior addresses, vehicle ownership or cohabitants.

Knowledge-based authentication quizzes can be posed as multiple-choice questions, with incorrect answers offered as red herrings.

Dynamic, knowledge-based authentication uses public, private and proprietary databases to obtain information not typically found in an individual's wallet. It relies on these additional sources of info to present a changing set of questions that can be asked in person, over the phone or online—and that only the correct individual can answer. This can significantly reduce fraud risks—for instance, these types of authentication techniques have reduced certain types of fraud in the online banking channel by an estimated 30 – 40 percent.

EVALUATE: "Can I do business with you?"

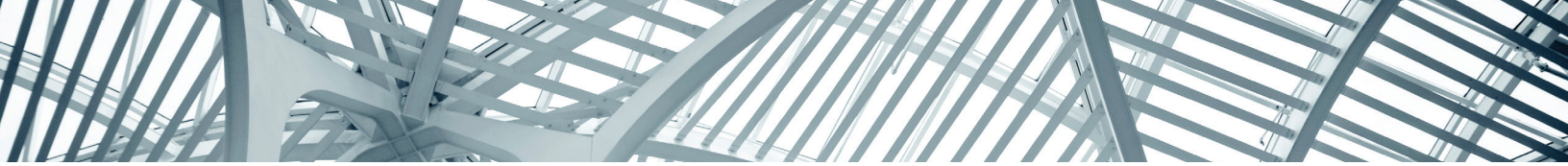
Identifying the risk potential of doing business with an individual can be accomplished in several ways: you can leverage public databases to verify a customer's date of birth matches his/her age range; determine if the address presented is high-risk, such as a post office box or a prison; or screen the customer's name against watch lists. This helps fulfill OFAC and USA PATRIOT Act compliance requirements and helps prevent fraudulent transactions.

ALERT: "Are you exhibiting high-risk behavior?"

Continuous evaluation of existing customers is critical to early fraud detection. One red flag for potential identity fraud can involve a new customer asking that something be shipped to an unknown address that differs from their billing address. This can occur across a range of industries, such as when a customer requests a replacement credit card from a bank or a monthly statement from a utility, or makes a purchase from an online retailer. It is recommended that you verify changes in address independently, as many consumers do not know their identity is stolen until after it has happened. Identifying changes in key criteria such as name, address and age, or uncovering the presence of a duplicate SSN or derogatory data, can also help you identify potential fraud before it happens.

Regular, ongoing customer identity validation is important because criminals continually devise new methods of fraud. They will also resurrect scams they retired months earlier or have used in other parts of the country to avoid creating patterns that can lead to detection.

LexisNexis®



Knowing Your Customers is Key to Mitigating Risk and Enabling Business

No matter the industry, all organizations have a responsibility to protect themselves and their customers from fraud. It starts by performing due diligence throughout the customer lifecycle via an effective customer identity management solution. In addition to mitigating fraud, this can also provide a competitive advantage. Knowing more about your customer can help you achieve multiple business objectives, from improved service delivery and brand reputation, to more effective product placement and increased profitability.

And knowing more doesn't have to mean asking more. By using solid identity verification methods and knowledge-based authentication to establish the identity as part of your customer identity management solution, you can select only the measures necessary to reach your desired level of assurance for onboarding new customers and reduce the risk associated with future transactions. This provides greater security for you and your customers—without increased friction.

Learn more about
Customer Identity Management.
Visit http://idmanagement.lexisnexis.com

LexisNexis®