pipl

Verifying Trustworthy New Accounts and Customers

It’s a problem

Criminals not only take over existing accounts, they open new accounts for establishing banking relationships or as “mule” accounts for holding money stolen from compromised accounts. According to an Information Security Group study, **85% of financial institutions*** reported experiencing fraud in the account opening process.

Common Approaches

Fraudulent identities and identity theft lie at the root of account-opening fraud. Traditionally, stolen PII and readily available social media profiles have been used to fabricate synthetic identities or impersonate legitimate account holders. In a disturbing shift, Javelin Research reports that criminals are now directly contacting victims through text, calls, or email to trick them into voluntarily providing data that will be used to scam them. Fraud management systems have a difficult time determining when a trusted customer is, in fact...not.

Truth Starts with Better Connections

Verifying an account holder requires more than identity data alone. It requires visibility into how that data is connected—and has evolved over time—with corresponding corroboration from multiple sources. It requires access to billions of global identifiers and the ability to analyze trillions of interconnections between them. Fraud prevention and management systems lack this crucial visibility and capacity. **Financial organizations need a way to identify trustworthy customers when an account is established so they can preempt fraudulent accounts and prevent fraud-related damage.**

The Impact

LexisNexis data shows that 1 in 7 new account creations are fraudulent. In fact, one large Asian bank found that 70% of credit card lending fraud cases came from what appeared to be “trusted” customers.	What is your organization’s strategy for identifying trustworthy new accounts and avoiding fraudulent accounts before they do damage?
According to RSA, almost half (48%) of all fraud involves accounts that are less than 24 hours old.	How quickly can your organization validate “trusted” customers’ identities?
For every dollar of fraud lost, U.S. financial services and lending companies now incur an average of $3.78 in costs.	What are fraud losses, compliance costs, and the cost of false declines costing your organization?
According to Javelin, one-third of identity fraud victims say their financial services providers did not satisfactorily resolve their problems, and 38% of victims closed their accounts.	How is fraud affecting your customers’ experiences of your institution?

Good News

Leading banks and financial services companies realize that if they can detect trust at the beginning of the account life cycle, they can significantly reduce the high costs of fraud and customer friction. Pipl provides more than 3 billion online identities with email, mobile phone, and social media data. Compiled from global identity data collected, corroborated, and connected over two decades, Pipl enables financial teams to quickly and easily make trust-based decisions about the people behind new accounts.

ISMG, The State of Digital Account Opening Transformation, March 2020