



Detect Fraud Before it happens with iSpyFraud

Sixty-two percent of companies were subjected to attempted or actual payment fraud in 2014¹. As the payment processing landscape continues to evolve, the opportunities for fraudulent activity will as well; with the expected rise in credit card use and the advance of mobile payment technology, it is predicted that the need for cyber security around payment processes will only increase.

iSpyFraud's software allows a merchant to anticipate and defend against fraudulent activity. Merchants can configure extensive filters to detect suspicious transactions before they're approved, and additionally, are provided with enhanced reporting capabilities that give them access to all the information they need to root out fraudsters for good.

How does iSpyFraud Work?

With iSpyFraud, merchants will have the ability to:

- Set rule-based parameters for transactions, defining such things as transaction volume per user, maximum amount charged in one transaction, and more
- Quickly and easily review transactions in any state, whether approved or not
- Access accurate and consolidated reports detailing the ins and outs of each transaction

Who Needs iSpyFraud?

Although most businesses could benefit from advanced security when accepting payments, some merchants are particularly prone to fraud:

- Merchants in what would be considered a high-risk business, including but not limited to electronics, subscription-based sales, weapons, fantasy sports, online gambling, and financial consulting
- Merchants who process a high volume of transactions, particularly card-not-present
- Merchants with international clientele

1. Association for Financial Professionals, "Payments Fraud and Control Survey: Report of Survey Results," *chase.com*, accessed September 2015. <https://www.chase.com/content/dam/chasecom/en/commercial-bank/executive-connect/common/document/afp-payments-fraud-results.pdf>