RISK MANAGEMENT

A multi–layered approach to payment fraud prevention

Fraudsters are becoming increasingly sophisticated and more efficient in identifying and exploiting vulnerabilities. As a result, merchants are paying more per dollar of fraud and losing a significantly higher percentage of revenue to fraud than in past years, with large ecommerce merchants and international merchants taking the hardest hit.[1]

Digital River has been helping online merchants identify and fight fraud for more than 20 years, running thousands of ecommerce sites worldwide. Through our Transaction Defender® payment fraud prevention system, we not only provide the tools you need, we also manage them for you. And, if we take on the Merchant of Record role on your behalf, we can also accept financial liability associated with fraud.

Flexibility

Because fraud methods vary greatly by market, channel and payment method, etc., it's important to find the right mitigation strategy and solution. While a variety of traditional fraud management methods have proven successful historically, Digital River continues to find new and innovative ways to protect online transactions across the globe. Our combination of a flexible screening engine, analytics, process controls and experience can help you accept more legitimate orders and minimize payment risk.

Global reach

When it comes to fighting fraud, there is strength in numbers. We continuously monitor all of our clients' sites so that we can identify fraud patterns from all over the world. You benefit from the community data gathered by our broad client base using Transaction Defender® to screen hundreds of millions of transactions originating from thousands of ecommerce sites in more than 190 countries.

24/7 expertise

We have dedicated global fraud prevention teams who are highly knowledgeable about what is or is not normal purchasing behavior. They are skilled at analyzing fraud trends and patterns around the clock and constantly developing proactive countermeasures to protect and maximize your revenue. Our experts will help you define your fraud processes and keep fraud under control.

Transaction Defender®

When you partner with Digital River, you're partnering with the most comprehensive online fraud detection and prevention system you can find. We'll help you welcome your customers in – while locking the criminals out.

1 Source: 2014 LexisNexis® True Cost of Fraud study

Protect your business and your profits from fraud

The Transaction Defender® payment fraud prevention system uses many different methods and tools to identify and prevent payment fraud. Transaction information gathered at checkout is filtered through each of these tools. If fraud is detected at any point, the transaction is stopped.

Fraud identification and prevention tools

- **Proxy piercing**: Detects when a proxy server is being used to circumvent common fraud controls, combating sophisticated fraud attacks effectively.
- **IP geo-location**: Identifies fraudsters operating in remote locations—possibly isolated from the law—by tracing IP addresses back to their originating locales or regions and comparing them to the transactions in process.
- **PC and device fingerprinting**: Detects and blocks the machines used by fraud rings to attack hundreds of ecommerce sites simultaneously. Transaction Defender® tags a machine, or set of machines, using a wide array of internet and browser session variables to prevent the machine(s) from perpetrating any further attacks against your business.
- **Customizable fraud thresholds**: Created the ideal screening levels to your unique business to process legitimate orders and block fraudulent orders. Thresholds can be tuned at a number of different levels, including company, market or even at the individual product level.
- **Intelligent fraud prevention engine**: Learns from past transactions, recognizes, and tags or blocks orders that contain data that has been previously found to be fraudulent. By learning from the past and using that information, Transaction Defender® dramatically reduces the need to manually review orders.
- **Rescreening engine**: Enables A/B Testing of new fraud rules with live—not historical—data. This feature silently tracks how new fraud rules might affect sales without actually implementing them and eliminates any risk to revenue.
- **Screening lists – blocked, trusted or neutral**: Compares each payment with lists of blocked or trusted payments where identified cyber criminals and validated payers are listed. You can also use a neutral list to identify transactions for testing purposes and let them pass.
- **Velocity checking**: Identifies and blocks potentially fraudulent payments by tracking how many times specific billing information has been entered within a set period of time.

Why are fraud rings so difficult to detect?

Cyber fraud rings use cheap labor and multiple computers to attack hundreds of ecommerce sites at the same time. Because these attacks are highly coordinated and the data entered always changes, it's very difficult to detect these attacks. However, the machines are a constant. Digital River PC and Device Fingerprinting can identify and shut down these computers, neatly preventing the attack in process.

About Digital River

Digital River, the revenue growth experts in global cloud commerce, helps companies of all sizes build and manage their online businesses, maximize online revenue, reduce costs and minimize risk. Founded in 1994, the company is headquartered in Minneapolis, with offices across the United States, Asia and Europe.

Unlock the value of Digital River to grow your business.

E: info@digitalriver.com
US: +1 800 598 7450
UK: +44 (0) 845 603 5070
TW: + 886 2 8173 1711
W: digitalriver.com/contact-us

digitalriver.com