

## MINIMIZE AND MANAGE ONLINE CREDIT CARD FRAUD

St. Gallen, Switzerland, June, 30 2011 – Card Payment Processing ranks amongst the most common payment methods used in e-commerce. In fact, card-not-present payments and online shopping go hand in hand, as they both offer an easy, fast and convenient way to reach customers worldwide and receive instant confirmation of the transaction. Yet, the recent news on security breaches in CitiGroup and Sony remind e-merchants of the vulnerability of the safety systems. These attacks have reportedly compromised the bank and card details of more than 100,000 customers, causing great loss to the companies hacked. E-merchants cannot help but wonder: how safe are the card e-payments reaching my web shop?

Surely, all major card issuers offer their own security systems (VbV, 3D Secure, etc), widely adopted by e-merchants and recognized by customers as a way to secure data transaction. Though highly accepted, few e-merchants realize the long-term implications of these systems to their businesses, such as the erroneous rejections from the card tools. Sadly, these procedures have little use in case of an extensive breach, as proved by the last DDoS attack to MasterCard website implemented by a renowned group of hacktivists showing their support to WikiLeaks founder. The attack resulted in the absolute fail of all verification tools, inability to complete direct credit transactions and, what's worse, negative impact on the brand image and loss of customer confidence.

Given the increasing frequency at which hackers are acting, it is vital for e-merchants to know now more than ever that the data introduced to conduct the purchase is not stolen, and that it will not result in a fraudulent chargeback.

E-merchants should not rely on pure luck when their businesses are at stake. Instead, they should make sure their businesses and customers are safe and protected with professionally-designed fraud-combating solutions that are easy to use and effectively adapt to new ways of fraud. However, it is especially important to stress the fact **that no solution can totally prevent fraud. E-merchants should therefore approach fraud combating from a different perspective: fraud cannot be completely erased, but it can certainly be minimized and managed.**

### How can CashRun help e-merchants?

CashRun has designed **CashShield, the ultimate fraud management platform**. CashShield's multilayered technology automatically screens all orders passing through a web shop with over 200 verification tests, which efficiently detect potentially fraudulent orders, assuring the maximum number of genuine orders is approved. Moreover, **CashShield offers the market's only 100% Chargeback Protection Policy** covering any undetected fraudulent order.

**CashShield's 200+ verification tests** allow a better assessment of the risk of fraud involved in orders passing through merchants' websites, and include

- **Geolocation Detection** to track, match and cross-reference IP addresses
- **Velocity Monitoring** tests to analyze card's expenditure and usage pattern
- **Device Fingerprinting** to detect fraudsters by the default information on the device, including a Proxy Detection System

**CashShield is helping a growing number of e-merchants increasing their revenue, by considerably dropping their chargeback rate and optimizing the risk credit card fraud present to their online sales.**

**CashShield is any online merchant's perfect partner** to manage the risk of fraudulent transactions thanks to its **innovative proven risk management algorithm**, which enables merchants to achieve an optimized return per risk level, so **e-merchants can focus on their core competencies and accelerate revenue growth.**

For additional information, please visit [www.cashrun.com/cashshield](http://www.cashrun.com/cashshield) or contact [marketing@cashrun.com](mailto:marketing@cashrun.com)

