

## Online Fraud and its Role in the E-Payments Merchants Initiative (EMI)

St. Gallen, Switzerland, August, 15<sup>th</sup> 2011 – During the past fifteen years, we have all witnessed the tremendous evolution of e-commerce and the online business from a restricted niche with great potential to what we know today, a full mature market. The sector has shown unexpected profitability and has reinvented and adapted itself to the new possibilities that its own, ubiquitous nature bring.

E-payments and the variety thereof available today are the result of this ever-changing scene in shopping habits and technologies. On the occasion of the Global E-Commerce Summit 2011 held May this year, major e-merchants and e-commerce organizations joined forces and drafted the **E-Payments Merchants Initiative or EMI**, a paper bringing together ten recommendations aimed at promoting discussion with all industry stakeholders, detecting the main cause of concern to e-merchants doing online business in and within Europe and giving directions to improve the European e-payment scene. The paper is currently under its third revision, and collects points of action in three main areas - cards, bank services and non-bank payments, suggesting valuable improvements. Most importantly, the EMI **makes a relevant mention to online fraud**, and calls for online authentication and e-identity interoperable options.

E-merchants know very well that online fraud these days is much more than chargebacks. Indeed, as specified in CashRun's latest [article](#), online authentication options have proved to be vulnerable, as shown by the recent attacks to major international corporations, while any form of online banking or non-bank payments is also subject to identity fraud. Anti-fraud tools have adopted several systems to detect identity fraud, the most common of which being Proxy Detectors, IP Detectors, Address Verification Tools and Device Fingerprinting. Though extremely useful, these systems do not protect totally against fraud, especially if used alone.

What can e-merchants do to stay protected? E-merchants therefore need to be aware of the limitations of apparently flexible in-house fraud combating solutions and the long-term implications that most of the third parties' solutions involve. The choice of fraud management affects both the customer experience in a web shop and the company's objectives in the long run, and as such it should be carefully considered.

At CashRun we believe that online fraud cannot be totally erased, but **fraud can certainly be minimized and managed**. Our **CashShield solution is the ultimate platform to manage the risks fraud presents to your online sales**. Thanks to **its 200+ automated verification tests**, CashShield ensures the highest number of genuine orders are processed, while protects e-merchants with **the market's only 100% Chargeback Protection Policy**.

**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 optimize revenue growth per their chargeback risk level**, so they 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)*

---

### About CashRun – [www.cashrun.com](http://www.cashrun.com)

CashRun was established in 2007 with the objective of supporting businesses' needs for effective and affordable online payment solutions. Since establishment, CashRun has had tremendous success with industries that are sensitive towards fraud, and continues to be at the forefront for solutions centering around e-commerce. With strong global presence and partnerships, CashRun supports businesses to develop firmly their core competencies, protect as well as maximize their revenues and growth, and minimize the risks credit card fraud presents to their operations.

