

## FRAUD PROTECTION GLOSSARY: UNDERSTANDING ONLINE FRAUD TO SUSTAIN YOUR BUSINESS

St. Gallen, Switzerland, May 31, 2011 - In the fast-paced world of online fraud protection, new changes occur at a mouse click. Fraud techniques evolve as fast as fraud protection tools develop, making it a real challenge for e-merchants to keep up with the different fraud trends and the protection methods available in the market. Yet this information is vital to keep online businesses protected and secure growth. Unfortunately, learning about fraud trends and the ways to combat them without professional advice leaves e-merchants one step behind almost all the time: by the time e-merchants learn how to deal with a certain fraud method, fraudsters are already attacking with a brand new technique.

In its commitment to support e-merchants and e-commerce professionals, CashRun has compiled the following glossary which offers an ample vision of the established and also the most recent terms and acronyms present in the fraud protection industry. The selection includes definitions and detailed explanations of verification tests and fraud protection features, aimed at bringing a fundamental understanding on fraud detection, which is essential to attain long term viability and sustainability of any online business.

**CSC Card Security Code:** Data cryptographed on an American Express card's magnetic stripe that protects data integrity and reveals counterfeiting or any other alteration. Referred as CVV for MasterCard cards

**CVV - Card Verification Value:** The Card Verification Value is divided in two types: the magnetic-stripe data and the printed security features. The first refers to the cryptographed data on the card's magnetic stripe, whereas the second one refers to the three-digit code usually printed at the back of any credit or debit card, which is requested when making online purchases, and must not be stored by merchants.

**Chargeback:** A fraudulent chargeback occurs when the card holder, alleging an illegitimate reason, contacts the issuing bank and orders the cancellation of the payment done online. E-merchants deliver the goods or services, but never get the payment. Even though e-merchants can claim the payment back from the holder's issuing bank, the success rate of this procedure is very low. Apart from the loss of unpaid but delivered goods/services, merchants dealing with chargebacks have to bear hidden costs associated with fees and penalties levied by banks; costly, ineffective and time-consuming in-house verification systems; and loss of potential customers due to the rejection of genuine orders. Therefore, staying protected against fraudulent chargebacks is vital to achieve business growth in any online business.

**Customer Profile Analysis:** Refers to the analysis done on the information a customer introduces on a merchant's web shop. Such analysis takes several factors when formulating a profile for each of a merchant's customers, including the e-mail address, origin, discrepancies, shipping location, payment method, IP address, device used for purchase, nature of purchase (nature, volume, frequency), and personally identifiable information in order to create the "identity" of this particular customer and determine the risk of fraud that this customer might perpetrate.

**E-Identity Profiling (EIP):** Set of diverse and ideally automated tests which help fraud protection solutions assess the risk of fraud involved in every order passing through a merchant's website. These tests might include Email Validation, Email Provider Checking, Global Telephone Directories, Global Address Verification Directories, Global Diverse Verification Services, and Global Identity Document Verification.

**E-mail Provider Checking:** Email providers are companies that provide e-mail connection and services to individuals and organizations. These services can be free or paid. An Email Provider Checking will allow e-merchants to verify the validity of a given e-mail address.

**Extensive Chargeback Database:** Fraud protection companies keep thorough databases compiling extensive data on past and current chargebacks, so any matching reference between an order and any data kept in that base can alert on a new chargeback.

**Fraud Statistical Training:** Relates to the training provided by fraud protection companies to their staff in order to enable their fraud officers identify fraud trends from studying the statistics from key findings of the fraud analysis.

**Geo Location Detection:** Set of diverse and ideally automated tests which help fraud protection solutions assess the risk of fraud involved in a specific order passing through a merchant's website. These tests might include IP to Zip Code, IP to Billing Address, High IP Cross Referencing, IP Geo Location & Proxy Detection, and NPA NXX Area Code Web Service.

**Geographical IP Detector (GID):** A web shop or a fraud protection solution equipped with a GID can easily locate the real physical (geographical) location of the device, by tracking the IP Address.

**Global Address Verification Directories:** This feature enables fraud protection solutions compare the address introduced by the visitor with the existing address, detecting any fake data. It also helps e-merchants keep their customers easily reachable.

**Global Address Verification Services:** Global Address Verification Services enable e-merchants to verify the complete address of a consumer visiting their web shop, avoiding fake addresses, and assuring that the typed address is correct, so physical delivery (if required) will be made to the customer's real address, and will not be delayed.

**Global Identity Document Verification:** In the event of an order failing to pass the initial ID test, customers are often asked to send a copy of any identification card (passport, ID, driving license), which are validated using a Global Identity Document Verification. This procedure helps e-merchants determine whether the ID used is real, and belongs to the customer as claimed. Document Verification techniques include factors as font type, lamination, holograms, position of picture and fingerprints, issuance, validity and numbering checks among many others.

**Global Telephone Directories:** This feature enables fraud protection solutions compare the telephone introduced by the visitor with the existing telephones, detecting any fake number, and ensuring visitors introduce their true contact phone number.

**High Risk BIN Transaction:** Every credit or debit card is identified with a 16-digit series which is associated with the Major Industry Identifier or MII. As such, Visa cards numbers will always begin with 4, American Express with 34, Maestro with 5 and so on. Analyzing the digits introduced by a visitor to a web shop enables e-merchants to filter out those fake or non-existing cards.

**High Risk IP Crossing Referencing:** Refers to the ability within fraud protection solutions to signal orders associated with high risk trends. This feature matches high risk IP addresses to high risk countries, or blacklisted IPs in the company's database which had previously experienced chargeback. As such, the true IP will be crossed-referenced to the databases and blocked should the results return negative.

**Historical Purchasing Pattern:** Ability to analyze current and past information and track any change in the shopping habits of the visitor and the payment method used, in order to detect any sudden alteration which might translate into fraud.

**IP Geolocation:** Geolocation systems can detect the country or even the city where a visitor to a website is, just by tracking the IP Address and determining the visitor's real-world geographical location.

**IP to Billing Address:** Process which matches a specific IP Address to the customer's billing address. The results will show if the customer's computer is really in the area claimed by the customer.

**IP to Country:** Process which matches a specific IP Address to a country, normally using databases which act as telephone directories. The results will show if the customer's computer is really in the country claimed by the customer.

**IP to Zip Code:** Process which matches a specific IP Address to a zip code, normally using databases which act as telephone directories. The results will show if the customer's computer is really in the area claimed by the customer.

**MCSecureCode:** Program designed and applied exclusively by MasterCard for MasterCard and Maestro debit and credit cards in order to further ensure online transactions made using a MasterCard or Maestro debit or credit card only at participating web shops. Cardholders are required to pre-register at MasterCard website, and to verify their identity before accepting the transaction.

**Multi-Merchant Transaction Database:** E-merchants compile and share information on past and current fraudsters and fraud techniques. By checking these independent, unbiased databases, online merchants are able to further sharpen their fraud-detection searches.

**NPA NXX Area Code Web Service:** NPA stands for Numbering Plan Area, that is, telephone area code. NPA-NXX codes refer to the combination of area codes (NPAs) and local exchanges or prefixes (NXXs). The combined code may contain up to 10,000 telephone numbers that are usually located within a specific geographic region. A NPA NXX Area Code Web Service enables instant identification of the geographical location of a specific phone number, and compares it with the geographical address introduced in the website.

**Online Fraud:** Any kind of fraudulent and/or criminal activity which is made via online services such as e-mail, messaging applications or websites. The most common form of online fraud affecting e-merchants are in the form of chargebacks, identity theft and credit card fraud.

**Payment Application Data Security Standard (PA DSS):** System designed by the Payment Card Industry Security Standards Council and adopted world-wide. This system prevents payment application from third parties from storing prohibited secured data. Companies providing payment processing solutions must also comply with the current 14 requirements on this system, as it is the case of CashRun.

**Payment Card Industry Data Security Standard (PCI DSS):** System which compiles common industry tools aimed at handle sensitive information in a secure way and prevent and react to any security incident. As a worldwide standard it applies to all organizations that hold, process, or exchange cardholder information. As PCI DSS constantly revises and changes its tools, online merchants need to revise their compliance every year. Currently, there are 12 requirements included in the standard. E-merchants accepting or processing card payments must comply with PCI DSS, and so must their fraud-prevention solutions.

**Payment Source Analysis:** Examination of the payment method used by the customer in order to better detect a fraudulent method (i.e., fake credit card) or any other dubious payment source (bank account mismatch, stolen pre-registered account, etc).

**PIN Transaction Security (PTS):** PIN Transaction Security combines several evaluation requirements managed by the Payment Card Industry Security Standards Council for PIN acceptance Point Of Interaction (POI) terminals.

**Product Risk Analysis:** Research of the products sold by the merchants in order to determine the risk level of each product or product group, and rate them accordingly. For example, intangible products will carry a higher risk due to the fact that there is no physical shipment and the transfer of ownership occurs within minutes, which leaves the door opened to chargebacks. Fraud protection solutions for example CashShield adjust to each product's risk level and optimize the risk involved for the merchant as a whole.

**Product Risk Segregation:** Product Risk Segregation is a spectrum on which the different risk levels are applied, for example, within intangible goods there might be high risk intangible goods and low risk intangible goods. Product Risk Segregation comes right after Product Risk Analysis. CashShield solution carries out these two products over and over again as risk can change overtime.

**Proxy Detection:** A proxy is a firewall system that replaces the IP address of a host with its own IP address. Proxies are often used by fraudsters to prevent their real IP addresses from being located. A proxy detection system simply detects whether a user's IP Address is an owned IP or a proxy.

**Risk Score Assignment (based on GID and EIP):** score assigned to a particular order, based on the results compiled by automated tests analyzing the visitor's geographical location and the e-Identity Profile.

**Risk Profile Assessment:** Set of diverse and ideally automated tests which help fraud protection solutions assess the risk of fraud involved in a specific order passing through a merchant's website. These tests might include High Risk BIN Database, Risk Score Assignment based on GID and EIP, Product Risk Segregation, Extensive Chargeback Database and Fraud Profiling Statistics.

**Risk Trend Analysis:** Set of diverse and ideally automated tests which help fraud protection solutions assess the risk of fraud involved in a specific order passing through a merchant's website. These tests might include Historical Purchasing Pattern, Payment Source Analysis, Fraud Statistical Training, Multi-Merchant Transaction Database, Velocity Monitoring and Product Risk Analysis.

**SSL (encryption):** SSL stands for Secure Socket Layer, and refers to a world-wide Internet protocol that encrypts the channel between a web browser and a web server to ensure the privacy and reliability of data transmitted over this channel. The industry highest standard now runs at 256-bit encryption, which rules all CashRun solutions.

**3D-Secure:** 3D Secure (3DS) is the program jointly developed by Visa and MasterCard to combat online credit card fraud. Cardholders introduce their password to verify their identity whenever they make an online purchase. E-merchants willing to offer this security service to its customers must be registered as a participating merchant in the program. Only cardholders registered at Verify by Visa or MasterCard SecureCode can actually be requested to verify their data when purchasing online.

**Velocity Monitoring:** This feature analyzes the pattern in a credit or debit card usage. A sudden change in the usual pattern might mean a fraudulent use of the card.

**VbV Verified by Visa:** Refers to the program designed and applied exclusively by Visa for its debit and credit cards in order to further ensure online transactions made using a Visa debit or credit card only at participating web shops. Cardholders are required to pre-register at Visa website, and to verify their identity before accepting the transaction.

The above glossary gives e-merchants an idea about the diversity of online fraud and different techniques to help prevent it. Unfortunately many fraud protection solutions simply focus on one of the features described above, and as a result tend to reject any order which might look potentially fraudulent. This not only creates a negative customer experience, but also prevents e-merchants from achieving full business growth by rejecting genuine orders.

Therefore, effective fraud protection tools must be designed and implemented as comprehensive systems which detect and unmask only real fraudulent orders as fast as possible, and adapt to new ways of fraud, helping e-merchants stay protected and focus only on the potential customers who will bring revenue growth.

### **How can CashRun help?**

At CashRun we believe merchants should only concentrate their focus on what they do best – business growth, leaving the rest to us. To ensure growth through verified transactions, the committed CashRun team has designed its innovative solution CashShield, a state-of-the-art fraud management solution which combines real-time order verification with a unique 100% Chargeback Protection Policy. CashShield allows merchants to:

- **Gain speed and customers**, by achieving real-time automated order verification, with its unique multilayered technology that screens every order with over 190 verification tests, signaling for any potentially fraudulent order in seconds
- **Protect their business** with CashShield's unique 100% Chargeback Protection Guarantee, reducing the risk of loss due to fraudulent chargeback to zero
- **Stay ahead of the competitors** by constantly updating the verification system, adding new parameters to adapt to the newest and most sophisticated forms of online fraud

**With CashShield, merchants and partners can cease worrying about the number one risk of doing business online – frauds and chargebacks. Balancing risks and revenue growth, merchants can focus on improving their core competencies, operational capabilities, and expansion plans.**

---

**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.