FRAUD FACTS

Fraud Advisory Panel

Issue 22 April 2014

INFORMATION FOR ORGANISATIONS

E-commerce risks to online retailers

With more businesses trading online, new scams have emerged as fraudsters target both e-commerce start-ups and more-established businesses. This factsheet highlights some of the most common scams targeting online retailers and provides advice on how to stay protected.

Introduction

Trading online is now a way of life for most retailers. It enables business to be transacted on demand 24/7 and reaches a worldwide pool of customers.

It also creates a number of security issues for you and your customers. Being aware of these risks and taking appropriate steps to reduce them is crucial to your business's long-term success.

One major risk to online retailers of all sizes and types is fraud. This factsheet highlights some of the most common online frauds that affect retailers and provides advice on how to stay protected.

Card not present (CNP) fraud

Card not present (CNP) fraud is a significant risk for online retailers (including those selling on eBay), and especially for small businesses.[1] It occurs when a stolen or fraudulent credit or debit card is used to buy goods and services from a business over the internet.

Losses can seriously impact revenue as dispatched goods, chargebacks (refunds) and postage fees may be irrecoverable.

When an online transaction is processed, authorisation is sought from the card issuer. The issuer checks that the card has not been reported lost, stolen or compromised and that there are sufficient funds available in the account. It does not check that the customer is the genuine cardholder. This means that if a transaction is later found to be fraudulent the retailer is often liable for the full amount of the transaction (called a 'chargeback'). The time limit for chargebacks can vary, but it can be up to six months.

There are a number of tools available that can be used to protect against CNP fraud. *Financial Fraud Action UK*[2] recommends the following.

- **Address Verification Service (AVS):** this service compares the delivery address with the billing address held by the card issuer. When the payment is processed it will return a successful match, partial match or failed result.
- **Card Security Code (CSC):** this is the three-digit security code on the back of Visa, MasterCard and Maestro cards, and the four-digit code on the front of American Express cards. Most Payment Service Providers (PSPs) require entry of the CSC in order to protect against fraud.
- **3D Secure** (MasterCard SecureCode, Verified by Visa and American Express SafeKey): this protects participating retailers against certain chargebacks (including those arising from fraudulent transactions) on credit and some debit card transactions by passing liability to the card issuer. It is important to check which transactions are covered as some card types are outside the scope of protection (eg, corporate cards).
- **Industry Hot Card File (IHCF):** this is an electronic file of payment cards that have been reported lost, stolen or compromised. Talk to your card acquirer or PSP for more information. Other alerts (such as TC40 and SAFE notifications) may also be available.

Other fraud prevention measures are also available. These include (but are not limited to) the following.

- **Fraud prevention databases:** these maintain an in-house database of prior fraud attempts and chargebacks. Alternatively you can subscribe to a third-party fraud prevention database. Use this information to help process (approve, reject or review) transactions (see next bullet).
- **Transaction monitoring and analysis:** use these techniques to stop or flag unusual and/or risky transactions such as high-value and/or repeat transactions taking place outside normal business hours by new customers; suspect orders from existing customers that are not consistent with their normal purchasing history; or orders originating from specific countries, IP addresses and/or card Issuing Identification Numbers (IIN) that are the first six digits of a card number.
- **Insurance:** insure high-value goods before delivering them to protect against fraud and loss.
- **Monitor deliveries:** do not deliver goods until payment has been received. Use a service that allows you to track the order and obtain proof of delivery. Keep a record as this can be useful if a chargeback is received. Fraudsters often request delivery of physical goods to an address that differs from the cardholder's billing address. Always do what you can to verify a delivery address before sending goods.
- **Common sense:** if you have any doubt about a transaction, perform additional checks (such as calling the customer to confirm the order) or do not accept it.

If selling on eBay look into PayPal seller protection which can provide extra safeguards against potential losses due to buyer claims, chargebacks or reversals. Online auction 'help' pages also provide many tips and hints on selling safely to avoid common buyer scams. For example, do not process payments outside the auction scheme rules, such as by bank wire or money transfer.

It is always advisable to contact your card acquirer or PSP for additional help and advice on preventing CNP fraud.

High-risk countries

Small online retailers should consider whether or not to accept international orders. It is always more difficult to retrieve goods once they have left the country. Your card acquirer or PSP should be able to give you a list of high-risk countries and provide advice about how to block such orders via your merchant administrative interface. Here are some questions to ask when processing an international order.

- Does the consumer's Internet Protocol (IP) country or origin differ from the postcode provided?
- Is the country high risk?
- Does the billing address vary considerably from the delivery address?

[1] Federation of Small Businesses (2013). *'Cyber security and fraud: the impact on small businesses'.*

[2] Financial Fraud Action UK coordinates fraud prevention activity by the financial services industry in the UK and works in partnership with The UK Cards Association.

Other common online frauds

Retailers can be exposed to other forms of online fraud, including (but not limited to) the following.

- **Customer dispute fraud:** a customer who has paid by credit or debit card claims that the goods have not arrived (despite the retailer posting the order to a verified address), and submits a chargeback request to their bank. Avoid these disputes by always keeping a record of orders placed, payments made and delivery receipts. Contact your card acquirer or PSP for further help on the chargeback resolution process.
- **Online corporate identity theft:** a fraudster steals your business's identity to gain instant recognition online by using the same (or similar) name and brand, company registration number and/or website domain name. The fraudster may also offer payment options and promotions in order to take orders that will never be fulfilled. Prevent this by periodically searching for your business name and registered company number online to see if your organisation's identity has been compromised. See our separate factsheet on *Corporate Identity Fraud* for more information.
- **Account takeover:** an employee responds to a spoof email and unwittingly discloses user credentials that are then used by a hacker to hijack your company's online account(s) for services such as online banks, e-wallets or auctions.
- **Internal (employee) fraud:** an employee refunds (credits) a family member's credit or debit card rather than the cards that belong to the genuine customers, or changes settlement bank account details and redirects profit to an unauthorised account.

Reporting fraud

- For CNP fraud contact your card acquirer or PSP and follow their advice.
- If you think your business has been the victim of an online scam or fraud report it to Action Fraud, the national fraud and internet crime reporting centre.

Protecting your business

DO:

- ✔ Select a trusted and reputable PSP. Make sure you fully understand your contract and the services offered to help protect against chargebacks and scams.
- ✔ Follow the merchant (retailer) rules and procedures recommended by your card acquirer or PSP.
- ✔ Have information security and anti-fraud policies in place and review them regularly.
- ✔ Keep firewalls and security software (such as anti-virus, anti-phishing and anti-spyware) up to date.
- ✔ Conduct penetration testing on your website to see how secure it is. Make sure any issues are fixed promptly.
- ✔ Ensure your payment processes are secure and meet with PCI-DSS requirements.
- ✔ Make sure that your business follows the principles of the Data Protection Act and best practice. Visit the Information Commissioner's Office website for more information.
- ✔ Consider introducing additional security measures such as those recommended by Financial Fraud Action UK.
- ✔ Conduct enhanced checks on high-risk/value orders and new customers. Consider following up with a welcome email or letter containing a verification code that can be entered online to verify a delivery address, especially for high-value, mail or telephone orders.
- ✔ Verify customers using registered details and by cross-checking these with public telephone or postal directories and/or credit reference agencies.
- ✔ Keep lists of good and bad customers and suppliers (eg, customers who submit multiple chargeback requests or suppliers who do not deliver on time) and cross-check these against new orders.
- ✔ Always keep records of sales and delivery receipts. These can provide valuable proof in chargeback disputes.
- ✔ Make fraud prevention part of your overall training strategy, starting with your induction programme. Provide staff with regular updates on an ongoing basis.

DO NOT:

- ✗ Assume your PSP will manage fraud on your behalf. Tools are provided and they should be used to prevent fraud and manage chargebacks.
- ✗ Ignore 'red flags'. Ensure that any risks specific to the business are adequately addressed.
- ✗ Accept payment for goods by cheque or bank/money transfer when dealing with customers you do not know or trust. Always use payment methods that give you adequate refund protection.
- ✗ Introduce overly generic training. It may be necessary to tailor training for different roles within your business.

Choosing a Payment Service Provider (PSP)

When choosing a PSP it is important to check that it is reputable, regulated and secure. Here are some of the questions that you need to ask.

- Is web-based administrative access protected securely with a strong password and Two Factor Authentication (2FA)? Ask for a key fob and extra protection when you log in.
- Is Internet Protocol (IP) lockdown available so that only the IP address associated with your computer is accepted upon login?
- Can you remove your staff's web-based access if there is an urgent need?
- Can you easily report on all refunds/credits, and any suspect or unusual amounts processed in a short time period?
- Is the PSP regulated by the UK Financial Conduct Authority and listed by Payment Card Industry Security Standards Council as a Level 1 service provider?

Note: only PSPs responsible for acquiring customer funds are regulated. All PSPs processing card information must be PCI DSS compliant.

Service providers offering CNP payment processing will give online retailers access to an administrative web-based portal. This portal is used to configure your web-based payment gateway, set up security features, initiate message authentication and process settlements/refunds. These sensitive actions must be safeguarded, monitored constantly and audited regularly to prevent account takeover and internal (employee) fraud.

Further information

Federation of Small Businesses
www.fsb.org.uk

Financial Conduct Authority
www.fca.org.uk

Financial Fraud Action UK
www.financialfraudaction.org.uk

Fraud Advisory Panel
www.fraudadvisorypanel.org

Get Safe Online
www.getsafeonline.org

Information Commissioner's Office
www.ico.org.uk

PCI Security Standards Council
www.pcisecuritystandards.org

The Fraud Advisory Panel gratefully acknowledges the contribution of Seona Devaney (Frisk Online) in the preparation of this Fraud Facts. Special thanks also to Financial Fraud Action UK for the provision of information.

Fraud Advisory Panel, Chartered Accountants' Hall, Moorgate Place, London EC2R 6EA.
Tel: 020 7920 8721, Fax: 020 7920 8545, Email: info@fraudadvisorypanel.org.
Company Limited by Guarantee Registered in England and Wales No. 04327390
Registered Charity No. 1108863

Distributed by