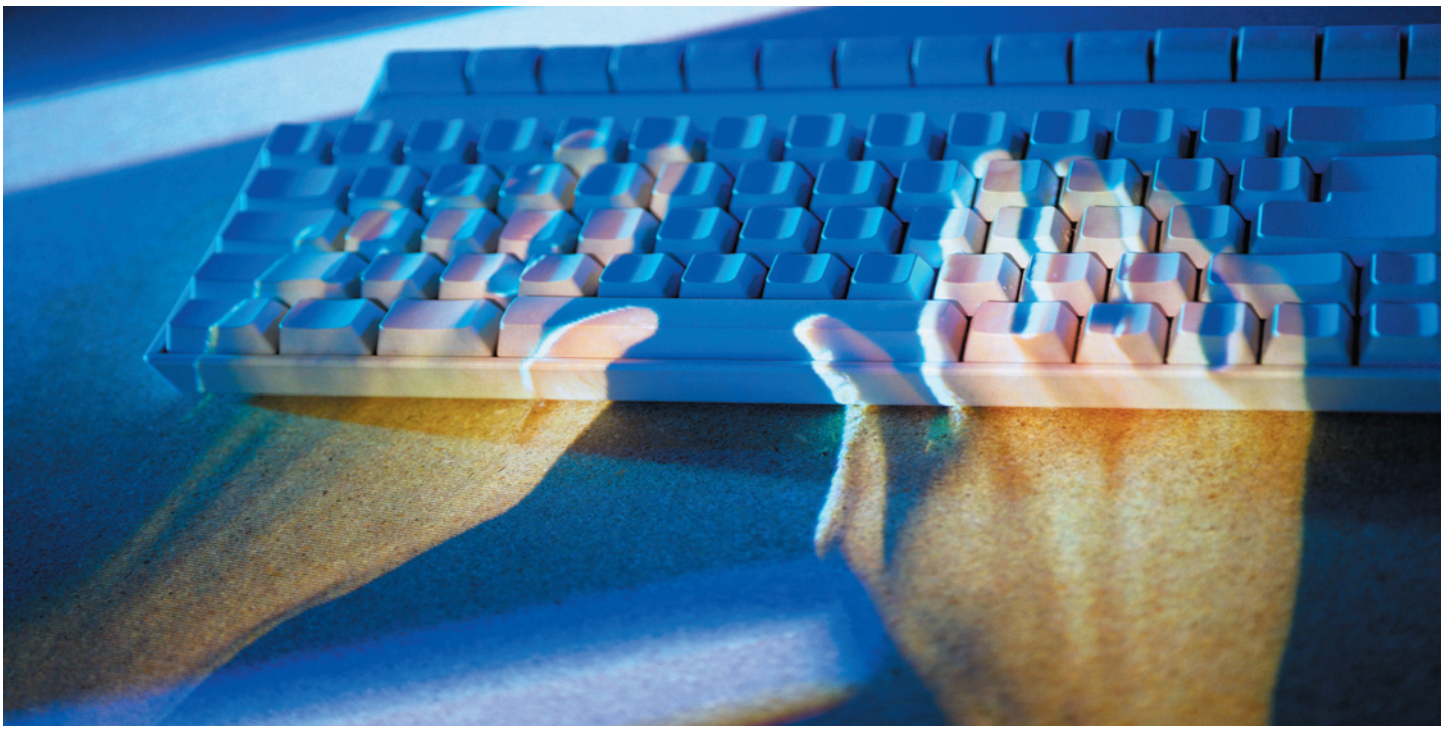
Proof positive

If a customer says they never placed an online order, what can a merchant do to prove otherwise?



As every organisation knows, there is a difference between taking an order and getting paid for that order. For companies selling goods or services online, the possibility of a customer saying they did not place an order – and blaming a technology glitch or even cyber-fraud – is a real problem.

The reason is straightforward, but the solution is not: Proving a transaction took place when neither party was physically present can be a challenge. What can a company do to prove a customer placed an order if he or she says otherwise?

In the world of online shopping, all transactions have the status of 'cardholder not present'. Credit card companies and banks originally introduced the concept in response to demand for phone-based transactions, such as ticket bookings, where the cardholder was not on the merchant's premises and therefore could not sign a receipt for comparison with his or her card. Since this makes the transaction less secure – the customer only having to know the cardholder's name, and the expiry date and number of the card to make a charge to it – card companies refuse to take responsibility for fraudulent or disputed transactions.

If a customer is adamant that he or she did not place the order, and there is no evidence of delivery of goods to the customer, the bank or credit card company makes a 'chargeback' and obtains reimbursement from the merchant of anything paid to the merchant. Even worse, the bank or credit card company may also make an administrative charge to the merchant for the transaction.

SELF-HELP

While the credit card companies have now developed schemes for authenticating cardholders online that reduce the risk to merchants (see box, *Credit where it's due*), these are still in the process of being rolled out and will not really tackle the problem until large numbers of customers have set up authentication information for their cards and merchants have adapted their servers to the systems. Until then, what can merchants do?

Ken Cowley, strategy director of payments technology group Etc, says that a company first needs to make its procedures transparent. "You need to be

Investigating integrity

ALTHOUGH the risks of fraud and failure in ecommerce transactions are substantial, very few companies are doing anything to alleviate the situation.

A study carried out in 2001 by research company Aspect Consulting in the UK, France and Germany, revealed that of 92 ebusiness directors:

- 60% rely on customer feedback to alert them to a transaction failure
- 71% do not have a system that enables them to manage the customer during a failure
- 63% are unable to measure the costs to the business of transaction failure
- 30% state that fixing the problem of failed transactions is not important
- 70% of respondents do not have a service level agreement to deliver a specific percentage of guaranteed transactions.

Credit where it's due

CREDIT card companies are finally stepping up to meet the challenge of ecommerce. To many merchants, Visa, Mastercard and other credit card providers have been sharing the benefits – but none of the risks – of ecommerce for several years.

Like phone transactions, online purchases are currently classified as "cardholder not present" transactions by card companies. Without the assurance of a signature, card companies regard the transaction as less secure and will not pay for it if it turns out to be fraudulent, meaning the merchant must instead. They do, of course, still take a fee if the transaction goes through. "They've been sitting pretty, leaving it all to the merchant and gradually increasing charges," says Ken Cowley, strategy director for payment technology company Etc.

Now, however, Mastercard and Visa are starting to roll out their own additional security schemes to merchants to improve card validation and authentication.

Visa 3D (or 'Three Domain') works by having the merchant install a plug-in on its transaction server (whether it is in-house or a third-party server). When a customer tries to use a credit card to pay for a transaction, the server checks with Visa's servers to see whether there are Visa 3D authentication details available for the card. If there are not, the transaction becomes a typical 'cardholder not there' purchase, but if there are, the merchant's server receives details from Visa on which server can authenticate the cardholder. The authentication server then requests login details from the customer, either via a password or an alternative such as a smart chip. If the result is valid, it digitally signs the authentication and passes it to the merchant's servers which can then approve the transaction.

Mastercard's UCAF (Universal Cardholder Authentication Field) and SPA (Secure Payment Application) installs a 'wallet' (basically, a web cookie) on cardholders' PCs to store extra authentication information. When the customer performs a transaction at a merchant's web site, the merchant's server combines information from the wallet together with information about the transaction to create a unique code that effectively identify the card, cardholder, transaction and merchant. If there is a dispute, Mastercard can decrypt the code for the transaction to see if it corresponds to the information specified.

Both systems are incompatible, and therefore require merchants to have different systems to authenticate different cards. In the long-term, however, they should reduce the chargebacks to merchants for fraudulent transactions. One advantage of the Mastercard system is that authentication is part of the overall transaction, so customers (or even merchants) who claim a transaction did not happen can have their claim examined quickly by simply seeing if there is an authentication code on Mastercard's servers for the transaction.

clear to the customer what constitutes a transaction. You need to say 'when you've placed an order, you'll receive an email that confirms the details'. And you need to have systems in place to notify you when emails can't be sent [so the customer can be contacted another way], for instance."

Ken Cowley, Etc: "You need to be clear to the customer what constitutes a transaction."

Analysts at IT market research company Aberdeen Group concur with Cowley. "Companies must think in terms of recording a 'contract' rather than the more popular, but very limited, concept of recording the 'data transaction'," says one Aberdeen analyst. It is not always enough to show that a customer placed an order: the customer can dispute terms of the agreement or pricing, so a merchant needs to show to everyone's satisfaction that the contract was entered into with everyone aware of the terms.

WEB LOGS

So the merchant should also record all aspects of the transaction and keep their details, but not just details of the sale. Web logs are a good starting point, but they only record what objects a web server sends to the customer's browser and what it receives in return. If a customer disputes that they saw a particular piece of information, it can be hard to show that the web pages they received contained the information, particularly if the pages have been redesigned since the transaction took place, or are dynamic. Other products, however, can monitor transactions and record all the information that can be useful in such situations.

One such product is Web Capture from document and content processing specialist, Tower Technology. "Web Capture records everything a customer saw in the course of a transaction," explains Adrian Foots, European product marketing manager at Tower Technology. "It captures everything between web server and web browser from when you

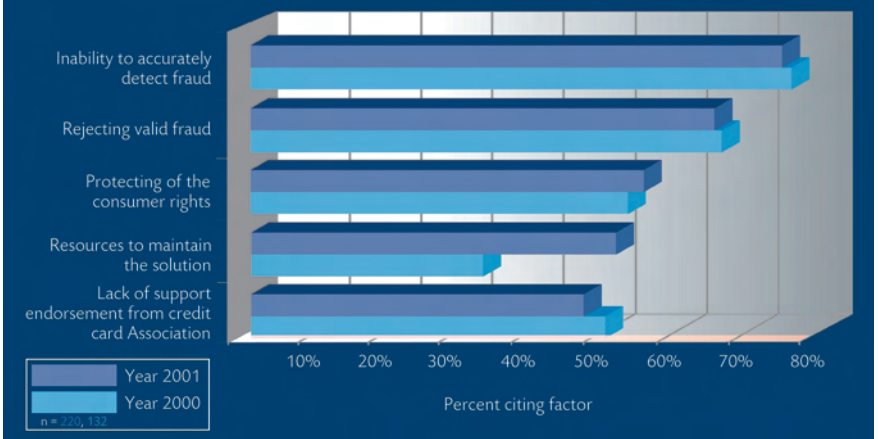
"Companies must think in terms of recording a 'contract' rather than the more popular, but very limited, concept of recording the 'data transaction'."

Fraud figures

EVERY year, e-payment company CyberSource surveys retailers to determine how much online fraud is a risk to them and how much it concerns them. The main results of 2001 were the following:

- 57% view online credit card fraud as a very serious or serious concern.
- The inability to accurately detect fraud remains the top concern, while the fastest-growing concern is in applying resources to maintain the solution.
- The impact of fraud is as big or bigger in online operations for the majority of organisations than in 2000.
- Fraudulent transactions account for 3% of online sales (on average).
- Expected revenue losses average 3% of overall revenue.
- The percentage of orders requiring human intervention has changed very little since 2000, and this intervention frequently inconveniences customers.

Concerns about fraud screening



Most companies have no idea whether their customer's online purchase, information transfer, or trade was successful or not.

go to a specific page until you finish the transaction or the transaction is abandoned." The software captures all the HTML, graphics and other objects that are sent to the browser, records its responses and when the transaction is complete, packages the data, digitally signs it and stores it in a repository. If a customer disputes an element of a transaction, the merchant can look at the data served to the customer to see what he or she did and saw.

"The main problems that are likely to occur are in complex products like insurance policies, where there are lots of contingencies," says Steve Naylor, vice president of marketing for Europe, the Middle East and Africa at Tower Technology. "Did the customer say they had treatment for a condition in exactly the same way as they would do if they were doing it offline, for instance? The cost can be huge," he warns, "because it affects pay outs and premiums. You need to be able to show that all the procedures have been followed."

Another product, Rainfinity's RainAssure, safeguards transactions in the event of infrastructure failures. At installation, the merchant simulates the various types of transactions possible on the site so that the system can understand what correct transactions should look like. John Kendall, business development director for Rainfinity in Europe, the Middle East and Africa, says the system then sits in front of the web server and monitors transactions as they come into the site, and determines if there are mistakes in them by comparing them with the learned transactions. It can then correct and continue transactions if a web server fails, for example, or notify customers of failure and the status of the transaction. Since it is monitoring the transaction, says Kendall, it can pass it to another web server to continue it, rather than make the customer start the transaction again.

John Kendall, Rainfinity: "The system can understand what correct transactions should look like."

LACK OF SYSTEMS

Despite the existence of products for transaction monitoring, research by Aspect Consulting suggests that even the bare minimum is being avoided in the majority of cases. While IT departments concentrate on trying to protect against the failure of their own systems, only 53% of those sampled monitor the end-to-end success or failure of a customer's online transaction. Most have no idea whether their customer's online purchase, information transfer, or trade was successful or not, leaving customers in the dark when a problem occurs.

Of those that do attempt to determine transaction success, nearly 60% of companies rely on the actual customer, rather than any management system, to alert them to a fault. And with 57% of them worried about fraud, many will be looking for more robust forms of reassurance soon.

CONTACT
Article by Rob Buckley
Email: rbuckley@infoconomy.com