

HEADLINE

The underworld of CVV dumping, carding and how to prevent it

STANDFIRST

Cyber criminals steal credit card information and then use forums and chat rooms to launder card data. This cost UK banks and businesses over £650m* in 2008. Julian Evans a leading identity fraud expert highlights the carding issues facing banks, businesses and consumers.

*APACS 2008 Fraud Report

CVV (Card Verification Value) is an authentication procedure established by credit card companies to further efforts towards reducing fraud over the Internet. The procedure is, in its essence, very simple indeed. It requires the card holder to quote the CVV number whenever a transaction is made online or over the telephone to verify the individual has the original card in their possession. The CVV code is in fact a very useful 'anti-fraud' security feature for "card not present" (CNP) transactions.

If you take a closer look at your card (both debit and credit) or have recently made a telephone or Internet purchase, you cannot have failed to notice the three-or-four-digit code on the back signature strip. The three-or-four-digit code provides a cryptographic check of the data embossed on the card. It's worth noting that the CVV code is not part of the card number itself. Most credit card companies have their own names for the CVV code, but the functions remain the same for all card types across the world; for example, VISA refer to the code as CVV2, MasterCard calls it CVC, and American Express calls it CID.

A closer look at the back signature panel of most VISA/MasterCards shows the full 16-digit account number followed by the CVV/CVC code, yet most banks in the UK and US only show the last four digits of the account number followed by the code. There are some important rules to remember for merchants who collect credit and debit card payments. CVV currently can be used in call centres where the card is directly keyed into a computer system which then instantly authorises the transaction. CVV can also be used on websites that use automatic authorisation. Outside of these instances they really can't - or shouldn't - be used or stored in any way. If a merchant stores a CVV number in the US, the fines that can be levied are very high, not to mention the loss of business and potentially being unable to process credit cards again – this could be potentially devastating. The simple rule of thumb for merchants is that a CVV code must never be written down, sent in an email or even stored on a database. These rules also apply in the UK.

The CVV anti-fraud system is not totally full-proof and no security system ever is. The biggest losers to CVV fraud are the merchants and the banks and credit card companies. Consumers are automatically protected by relevant statutory laws in most countries.

A positive CVV match might not 'assure' the consumer is the legitimate holder and most criminals know just how easy it is to skim a card and write the CVV number down. Even if the card is proven to have been used fraudulently, having the CVV code doesn't guarantee a merchant a chargeback. In fact, all the CVV code provides is just "another" 'anti-fraud' measure.

CVV numbers do appear to wear off quickly and are often unreadable after a short period of time. So you can see the problem customers experience when purchasing goods over the Internet or the telephone. One of the biggest headaches for identity thieves is when they are skimming cards (stealing the data from the magnetic stripe on the back of all credit and debit cards) they are now needing the CVV code, especially if they are purchasing goods online, over the telephone or in foreign countries. It is recognized that the CVV code does prevent fraudulent transactions from skimmed cards (a growing threat where Chip and Pin is being used, like in the UK and France – the USA does not use Chip and Pin, as is the case in much of Europe and Eastern Europe/Asia).

Carding – The merchant threat

'Carding' is often referred to as 'Card testing'. This type of fraud has been around for some time, but still not everyone is fully aware of it, or understands how it works. It is on its own, one of the most costly types of business fraud, even though in most cases the goods or services ordered may never have been shipped.

Card testing can usually be identified by observing large numbers of declined transactions which normally appear as a consistent pattern. Someone (not always fraudsters) attempt a number of transactions in the hope they will eventually get an approved transaction – this could mean that "someone" is card testing, but not necessarily. Card testing is usually done in small amounts (and in a specific pattern, as previously mentioned) as the tester only wants to find valid numbers that can be used for purchasing.

The card testing procedure goes through two different processes. These involve finding the real 16-digit card number and the expiration date to match. Fraudsters have identified a particular method in which they can fool both first line defence and neural behavioural fraud detection software.

By using a particular type of algorithm called 'Luhn', a fraudster can produce a number of valid credit or debit card numbers. Eventually the fraudster will come across a valid card number which they then follow up with a number of expiration date submissions until the card is approved. As with computer Trojans and viruses, a complex computer script is developed to produce automated queries into merchant payment systems. You can now see just how fraudsters fool complex anti-fraud detection systems as well as the banks and credit card companies.

What protection do we all have?

As is the case most businesses, no matter where they are in the world (and especially as the Internet is starting to fuel CNP and Card testing) nearly every business will be charged for every transaction, whether declined or approved. The number of card testers ranges in the tens of thousands of tests per day. The approximate cost for each transaction is roughly £0.15 so you can see the financial implications immediately. That said, leading financial institutions such as Visa and MasterCard monitor as best they can the various payment gateways where there are large volumes of cards declined. For most businesses, identifying the card tester and blocking the transaction using both First Lin Defence (FLD) and behavioural fraud detection software goes some way to reducing the financial risk.

A similar scenario exists for consumers, but the impacts are more of an inconvenience than any actual financial issue. The consumer might notice a credit card statement has unusual small amounts debited and/or the credit card company has called as they have noticed unusual patterns on the credit/debit card i.e. your card was used at say 3am and the amounts started small and then started to increase over a given time period. A favourite trick for fraudsters is to use your card in this way on gambling websites... so always keep a watchful eye to avoid finding yourself out of pocket.

Consumer cost is minimal, especially if you have used a credit card. Most credit cards are protected in the US and UK to a certain amount (see CCA and FCBA below); so if you spend over \$50 (US) or £50 (UK) you are automatically protected. At ID Theft Protect we refer to these as 'Credit Protection Levels' or CPLs, which incidentally have lowered in recent years. The thinking amongst security professionals is that the CPLs will start to increase as the costs and economic climate bites hard in the financial sector, and more importantly as CNP fraud continues to grow. Expect credit card companies to scrutinise every fraudulent credit card claim and expect refund delays and in some instances you might be refused the refund altogether - be warned!

Also you should be aware that even under the UK Credit Consumer Act (CCA) they are not obliged to refund you any loss if they suspect you have been negligent. This also applies in the US under the Fair Credit Billing Act (FCBA). Many people who contact ID Theft Protect ask us why debit cards are not protected the same way as credit cards. The simple truth is that they are, but it is left to the banks' discretion to refund any debit card, direct debit, cheque or bank fraud. The other issue often overlooked with banking fraud (this includes debit card fraud) is that fraudulent claims are handled much more slowly in the banking sector than with credit card companies; so you could be without access to your banking accounts and have the stress of recovering those stolen funds, which can last for several weeks, if not longer.

So if you happen to be a victim of, for example debit card fraud make sure you don't use your BILLS account to pay for anything online or when out shopping – keep that account separate. Why? The simple reason is that your mortgage, utility and insurance bills should go out of one account and you must avoid using the BILLS account for anything other than your primary bills.

Carders

Most “Carders” are aged between 13 and 20 and normally hang around Internet Relay Chat (IRC) carding channels with the purpose of buying and re-selling the bricks necessary for the scams. These “Carders” earn small amounts of monthly income, with many profiting from rip-offs. Outside of IRC rooms we have the money mules. These are much older than the “Carder Kids” but have the skills needed to turn virtual money into real cash.

The marketplace for carding is growing and will continue to grow. Some of the mules will use e-gold for anonymity and using wired cash can also provide the mule with security – more often than not the wired cash is irreversible. What might surprise you is that the mules actually transfer their ill-gotten financial rewards into legal bank accounts!

The carding costs vary dependent on the marketplace (by this we refer to the IRC forums and auction websites). Expect to purchase full credit card information for anything between \$2 -\$5 payable using e-gold. Furthermore, what will also surprise you is that most of the credit cards are bought by packs, something akin to drug smuggling.

The carding process is very simple. Some security professionals call the “carding process” a “substantial business model”; it doesn't matter whether the economic climate is good or bad, there is always a market for fraud and especially for carding if you have the business model and most importantly have built the trust on the auction site. The auction site is where it starts and ends with cyber criminals involved in buying goods from online shops and delivering them to the 'drops' which then forward the “goods” back to the cyber criminals who then sell the goods to the auction site.

Credit card dumps

The credit card dump is where a fraudster has stolen your credit or debit card information to commit financial fraud in your good name. The card information, for example, can be skimmed almost anywhere and at any time – some of the more popular skimming locations are shops, restaurants, railway stations, petrol stations and ATM machines. Worst of all, you might have no idea your card has been skimmed / cloned until you receive a phone call from your bank informing you of just that.

So when the fraudster has stolen your card information, what can they do with it? The most popular way to use your stolen card information is to sell the card information as 'dumps'. A dump file contains all the data that is stored on your credit card's magnetic strip.

Have you ever wondered how your credit card information is bought, sold or transferred? Have you ever wondered how someone uses your credit card information after it is stolen to commit fraud? There are a number of ways, but the preferred method is through using dumps. A dump is a file containing the data that is stored on a credit card's magnetic strip (see previous section). Dumps are one of the fastest growing frauds in the world today.

Dumps also allow the carder to dump card data onto absolutely anything that has a magnetic card. Now think about which cards use magnetic stripes – hotel room keys, discount cards, gift cards and other credit cards etc – think of the fraud possibilities. Laundering credit cards becomes very easy indeed. A fraudster who has the card information can simply use their own credit card and dump stolen data onto it to purchase anything in person. You might also say that it will prove more difficult to purchase in person; well it isn't. How many shops and restaurants do you know who compare the credit number printed on the receipt with the card itself? Actually no one does this. The credit card number is never printed in full (or not at all) on a receipt. The only solution here is for employers to keep an eagle eye on their staff.

A worthy trick for consumers to remember for your credit and debit cards, especially if your card is taken out of your sight or if your card has been skimmed (cloned) – cover the CVV code with a small piece of masking tape. If the card is tampered with then you will know about it and can take the appropriate steps to cancel the card. This is a very useful anti-fraud method, especially when you are away on holiday (which is when a fraud might well occur). Just hide all the CVV numbers on all your cards.

Carding costs

The actual costs involved in buying good card data varies and is dependent upon how many you buy. For example, buying the valid card numbers (you need to understand how to prove they are valid, which is by no means an easy task!) would probably be sold on a website like eBay for anything between \$250-\$450 per package.

That said, many websites are now validating the content that is posted, so being able to sell CVV dumps on reputable websites is becoming more difficult. Hence, forums and chat rooms (IRC) are where most buying and selling is done.

Search Google using some simple keywords: “CVV card dumping” and this will show up a whole list of the latest CVV dump opportunities. It is not an easy task to purchase any of these dumps as the mules are very careful indeed when it comes to selling – the main reason being 'trust' – they don't know you, so they could be chatting to a police officer.... You also need to understand their 'language' – by this we mean the 'text speak'.

What is the banking industry doing to stop card crime?

In the UK, the banking industry is engaged in an ongoing battle to combat card fraud. Some of these include the creation of the Payment Industry and Police Joint Intelligence Unit (PIPJIU) which was as a result of an amalgamation of the Fraud Intelligence Bureau (FIB) and the intelligence section of the Dedicated Check and Plastic Crime Unit (DCPCU). The core areas of responsibility for the PIPJIU are providing more efficient approaches to the collation and dissemination of fraud intelligence for police forces and being able to address all types of banking fraud, not just cheque and card fraud.

The UK also has the DCPCU which is fully sponsored by the banking industry. The unit is staffed by Metropolitan and City of London Police forces as well as banking experts. The unit focuses on serious and organized cheque and card crime and works with other law enforcement agencies across the UK and overseas.

Another UK initiative involves the retail industry. CardWatch is running retailer training programmes on behalf of the banking industry to assist point-of-sale staff identify and prevent card fraud. Additionally, retailers are investing in more intelligent fraud detection systems which identify unusual user behavioural patterns on spending – i.e. time, frequency and payment location, not just here in the UK, but also internationally as well.

Earlier this year Visa introduced a new type of credit card in an attempt to combat consumer identity fraud. The 'Keypad Credit Card' card, which is still being trialled, has unique features specifically designed to combat identity fraud; it looks exactly like a normal credit card and is powered by a battery that will last three years. The card has an LCD screen and 12-button keypad that can be used by the cardholder to input a PIN every time an online purchase is made.

Another bank leading the way in the fight against card fraud is Barclays. They offer a simple device called PINsentry. The PINsentry device for consumers is a new way to help their customers use Online Banking using chip and PIN technology. It changes the way you log in and make certain payments. In all instances the customer will need the hand-held card reader together with bank debit or authorised card to authenticate the individual's identity when setting up payments to someone new.

As you can see, banks are moving in the token and card reader direction, meaning customers have to carry a device with them everywhere they go to perform online or CNP transactions. These methods can be affective but some may find them an inconvenience to use. Some banks are also providing a 'call back' service on payments and deposits – a phone number of your choice is provided and the bank will call you to confirm payment or the deposit.

Lasting thoughts

Earlier this year there was evidence to suggest that fraudsters are actively and publicly spreading information (and mis-information) about other fraudster activities. A spammer (origin not known or provided in the public domain) was using an existing spam botnet to send messages about the Russian credit card trading (carder website) <http://carder.su>

Take a look, but be careful, because you don't know whether there are any malicious programs at work – other than the obvious card dumps on offer. Carder.su is a very popular website as at its maximum recently it had over 14,000 members logged in at the same time. If you want to take a look at another carder website take a look at <http://cardingworld.lefora.com/headlines/>

Will the banking and law enforcement agencies ever win the fight against banking and credit card fraud? Only you can decide that.