

Direct debit: making life - and fraud - easier

The Direct Debit scheme has revolutionised the way in which bills are paid, and has drastically cut the number of people who couldn't manage to pay their bills on time. Since 1995 the number of Direct Debit transactions has increased by a staggering 200 percent according to APACS. Furthermore, over 48% of the UK bill-paying population has declared Direct Debit to be their preferred payment method, with 74% of users agreeing that Direct Debit makes life easier and 80% of users believing it saves time. The ease of using debit cards to pay bills and use in store, over the internet and on the phone has certainly made lives easier and has probably contributed to helping those that are financially stable remain that way.

Additionally, there exists plenty of scope for the continued growth of both Direct Debits and Direct Credits, with Direct Debits expected to grow by a further 125% over the next eight years and Direct Credits by over 200%.

However, does this ease of use also come with an increased ability for others to use the system to their advantage? The introduction of chip and PIN provided increased security for consumers; and it is likely that many of the same consumers assumed Direct Debit and Direct Credit payments provided the same level of security. Unfortunately, they are now discovering this is not the case as fraudsters have found ways to target these kinds of payments and use them to their advantage.

It is easy to understand how thieves have used people's credit cards to make purchases in the past. They simply stole the actual cards and made purchases in store, over the phone or online. It was simple to get all the details necessary just by picking up a wallet. Most people don't realise that it is just as easy for fraudsters to get a hold of your details and use cards to make Direct Debit payments.

Often, fraudsters pose as legitimate customers with a full set of details. Because of the way the system works, when fraudulent payments are found, they are usually considered to be processing errors rather than a fraudulent transaction and are only recognised after the real person notices they are making payments for things they have not authorised.

So, how do they do it? Fortunately for the fraudsters there are an ever increasing number of services that can be purchased by regular Direct Debit payments such as mobile phone contracts. When purchasing a mobile phone the customer is required to take out a [Direct Debit](#) to pay for the cost of the phone and the contract. The checks that are currently in place to validate the details are relatively rudimentary and will often pass through validation systems. The "customer" leaves the store with a new phone and up to two years of free phone usage paid for with someone else's bank account details.

Unfortunately this type of fraud is only detected when the originating organisation or the customer's bank receives a complaint either because the payment has not been made or received, or because an unauthorised payment has been made or received. Although much fraud is believed to go unnoticed as fraudsters focus on high volumes of low payments (and individuals receiving misapplied payments are unlikely to draw attention to them), large unauthorised withdrawals have been recorded.

However, more organisations are becoming aware of this hole in the system and are looking for solutions to help keep transactions more secure. Direct Debit and Direct Credit fraud is possible because the systems in place to check on the accuracy of customer-supplied personal and bank information are currently limited to checking the format validity of bank account data. A solution to combat this kind of fraud would be to allow for these systems to cross reference and match the customer's details with their bank account details.

About the Author

Adam Singleton is an online, freelance journalist and keen gardener. He lives in Scotland with his two dogs.

Source: <http://www.tntarticles.com>