



Consumer Alert: Instant EFT online payments

The South African Reserve Bank (SARB) and the Financial Sector Conduct Authority (FSCA), in consultation with the Payments Association of South Africa (PASA), would like to issue a warning to consumers to be aware of the risks associated with the use of instant electronic funds transfer (EFT) online payment services offered at e-commerce stores (i.e. stores which facilitate the purchase and sale of goods and/or services via the Internet).

What is an instant EFT?

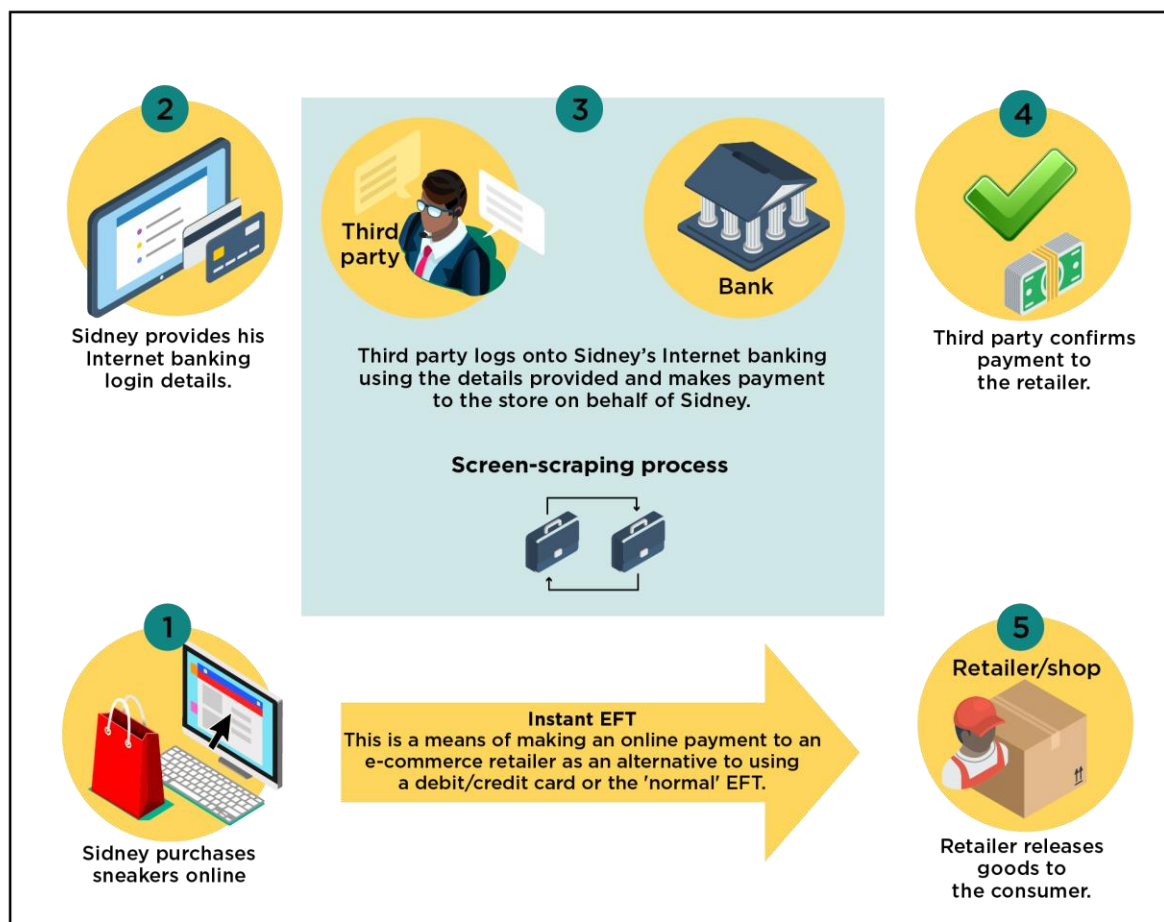
An instant EFT is a payment method offered by a third party, in partnership with e-commerce stores, which automates the initiation of payments for consumers to e-commerce stores and also provides immediate confirmation of payment to the e-commerce store to enable them to dispatch the goods or services purchased.

Instant EFT payments use a method called 'screen scraping', which makes it possible for third parties to access bank account data and automate actions on behalf of a consumer using that consumer's online banking access credentials. The access to the consumer's screen data is then used to facilitate payments.

Consider the following scenario:

Sidney wants to order a pair of sneakers for his son's birthday. He searches for an online clothing store and finds the perfect pair. He selects the size and colour, and clicks on 'Buy Now'. Sidney proceeds to the delivery details and payment page. Here, he is asked how he will make the payment, and selects the 'Instant EFT' option. Sidney is given a list of banks and is prompted to select the bank he uses. Immediately, he is redirected to a page with his bank's logo, and is required to enter his online banking details. He inputs his online banking username and password, and clicks on 'Submit'. Once he inputs the username and password, he is required to select the account from which he wishes to make the payment, and is then required to authenticate the payment via his mobile phone. The web page then moves to the payment confirmation page to inform Sidney that his payment was successful. Finally, he receives an SMS message from his bank alerting him that a payment has been made. Instant EFT benefits Sidney in that he can make purchases quickly and easily from any online store.

An example of an instant EFT online payment is illustrated below.



What are the risks to consumers?

The SARB, the FSCA and the payments industry do not support the use of screen scraping to effect payments, given that it exposes consumers to the following risks:

Data privacy

The method of using screen scraping to effect payments puts consumers' access credentials at risk of being compromised. Consumers have no control over how their credentials, and any other data or personal information, are accessed and used by the third party (e.g. account numbers and account statements can be stored and utilised without the consumer's knowledge or consent).

Fraud risk

Rogue entities might pose as third parties offering instant EFT services on fake e-commerce sites to capture consumers' access credentials for their bank's Internet banking websites. From there, such entities might impersonate the consumer and conduct any activity that the consumer would have access to on their online banking platform (e.g. making real-time payments to themselves, applying for a personal loan, increasing transaction limits, and ultimately initiating payments to mule accounts). Rogue entities might also access relevant data and personal information such as

account information and monthly statements from which fraudulent collections through debit orders might occur.

Breach of contractual agreements

By providing their Internet banking login credentials to a third party, consumers that use instant EFT products might be in breach of their banks' terms and conditions which regulate Internet banking. As a result, knowingly or unknowingly, consumers might be giving up their rights of recourse and any legal protection in the event of suffering fraud and/or subsequent loss.

Risk of financial loss and the goods purchased being lost

EFT payments are final and irrevocable in nature, and consumers are unable to lodge disputes to reverse a transaction in the event of the online store not honouring their agreement (e.g. not delivering the goods or delivering counterfeit goods). Consumers might also be held liable for the interest payable on such amounts when payment was made from their credit card account or overdraft facilities.

Tips for consumers

As the global economy experiences an increase in the use of electronic payments and online shopping, and considering the growing role of financial technology (fintech) in payments, online crimes are increasing. It is becoming even more important for consumers to educate themselves on the risks and benefits of using online means to make payments or order goods and services. It is also becoming exceptionally difficult for regulators and the financial industry alike to keep up with such crimes before a loss is experienced by either party.

We therefore encourage the following practices:

- Consumers need to be extra vigilant. They need to do all their checks, including contacting their banks for advice, before proceeding with something marketed and disguised under the premise of convenience.
- Consumers should use industry-supported solutions, like paying with their cards (debit or credit cards).
- Consumers should *not* share their Internet banking logon credentials with any third party.

Issued by: South African Reserve Bank, Financial Sector Conduct Authority and Payments Association of South Africa

Date: 26 November 2020