



AIB urges customers to be vigilant after payment fraud cases increase by 59% in July

- **Surge driven by a rise in text message and phone call scams**
- **Fraudsters have persuaded customers to withdraw sums of cash before arranging for it to be collected**
- **Customers urged to *'Wait a sec, double check'* before acting on any unexpected request**

AIB is warning that a growing number of customers are being tricked into sending money directly to fraudsters, or handing over security codes and even their bank cards and cash. It follows a 59% increase in payment fraud cases in July when compared to previous months.

Recent fraud intelligence has recorded a significant rise in convincing text messages and phone calls from criminals impersonating trusted organisations. Case reviews also show continued instances of fraudsters arranging the collection of customers' bank cards and even quantities of cash under false pretences.

Fraudsters are increasingly using sophisticated social engineering techniques to gain a customer's trust, before persuading them to transfer money, reveal security information, or hand over their card. Typically, customers receive a text message claiming to be from their bank or another trusted organisation such as a delivery company or Government agency. This text message is often followed up by a phone call from a fraudster who claims to be AIB staff, and who attempts to create a sense of urgency to convince the customer to act quickly.

Customers are being asked for security codes under the guise of cancelling fraudulent transactions. These codes are allowing a fraudster to enrol new devices and make payments from customer accounts. In other cases, customers are told that their account is compromised and they must move their funds to a so called 'safe account'. The caller will provide the customer with a new account, which is in fact controlled by the fraudster.

AIB has also seen cases where fraudsters have persuaded customers to withdraw sums of cash, before arranging for this to be collected at an arranged location or from their home. Criminals may claim the cash is required for an investigation, to protect the customer's funds, or to be lodged to their so-called new account. In some cases, customers have been advised to not tell legitimate staff the reason for their withdrawal or transfer. These claims are fraudulent. AIB and other legitimate organisations will never ask a customer to withdraw cash and hand it over for collection.

AIB is reminding customers that:

- We will never ask you to move money to a "safe account".
- We will never ask you to share one-time security codes, passwords or login details.
- We will never collect your card and PIN.

- We will never ask you to withdraw cash on our behalf.
- We will never ask you to delete the AIB Mobile App And not reinstall it or tell you not to access your accounts for a period of time.

Head of Fraud Intelligence at AIB, Harold Perez, said: “We are seeing a notable increase in the number of customers being targeted in sophisticated text message and phone call scams. Fraudsters continue to adapt their tactics and are becoming increasingly convincing in the way they target customers. We are asking customers to ‘Wait a sec, double check’, before acting on any unexpected request. A genuine organisation will never pressure you into making immediate decisions about your finances.”

“Fraudsters are highly skilled at creating a sense of urgency and trust. Our advice is simple: take a second to think before acting. Never move money to a so-called safe account, never share security codes, and never hand over your card, PIN or cash to anyone claiming to be us. If you're unsure, end the conversation and contact us directly using a trusted phone number. Taking a moment to pause could prevent significant financial loss.”

For more information on how to protect yourself from fraud, visit our Security Centre on aib.ie. Here you will also find our contact information, including our 24/7 fraud support line on 1800 24 22 27.

Media: will.r.goodbody@aib.ie or 086-8502204