ING Group	EUR Not Identifiable Loss | Euro
USD Not Identifiable Loss | US Dollar	EUR Not Identifiable Loss | Euro
BL0301 - Retail Banking	EL0201 - External Theft & Fraud
NL - Netherlands	Western Europe
Loss Event	Published in media 07 September 2019

ING Bank to pay customers compensation over QR code fraud via mobile banking accounts

On 7 September 2019, it was reported that ING Bank would compensate customers who lost money as a result of fraud using ING's own QR codes which was conducted via their mobile banking accounts.

ING offers account holders the option of using a QR code to link a second device to their mobile banking account. The perpetrators obtained ING account holders' account numbers, purportedly to pay them for goods sold online via the classified website Marktplaats. Using these account numbers, the perpetrators were able to generate an ING QR code using the ING mobile app on their phones, representing that they had the app installed on another device. The perpetrators sent the QR code to the ING customers, claiming that scanning the code would confirm the payment. In fact, by scanning the ING QR code sent to them by the perpetrators to the ING mobile banking app, the customers unknowingly activated the ING mobile banking app on the perpetrators' device, giving them access to their ING bank account. The perpetrators defrauded some ING customers of thousands of euros in this way.

The customers only realised they had allowed criminals to access their bank accounts when they saw that money had disappeared from their accounts. ING initially informed customers who lost money this way that it would not compensate them for the money they lost, as the customers themselves were responsible for the linking of third-party devices to their own accounts. ING said in September 2019 that it had become aware that hundreds of clients had been affected by the scam in recent months and it would compensate them as a goodwill gesture.

A spokesperson for ING said the bank had considered the linking process for customers' devices to be secure and very clear. As part of the process, customers were asked to enter the access code of their ING app and specifically asked if they really wanted to activate the app on another device. A report by consumer television programme Kassa in the Netherlands stated that in comparison with other banks' systems, ING's QR code system required fewer steps to link a device, making it vulnerable, according to kassa.bnnvara.nl.

The bank said it would implement additional measures to increase its customers' security in view of the fraud. In a new update to the app, to be released around 21 September 2019, the bank said customers would be alerted when they activated a new device, via information screens displaying for five seconds, that they were

allowing another device to access their account and conduct transactions in their account. Customers would have to state that they had not scanned a code received from a third party, were activating the app on their own device and were providing full access to their banking affairs. The update would advise customers to contact the bank immediately if someone requested their QR code.

ING said customers were not required to contact the bank to receive compensation and would be automatically contacted by letter in the week commencing 9 September 2019. ING did not specify how many customers were affected but said that the compensation was a “considerable amount” and that there had been a few hundred reports of theft using QR codes. ING advised its customers to be attentive when scanning QR codes.

Author: Pamela Swann **Published Date:** 09 September 2019 **Last Update:** 11 September 2019

O.R.X | News

ORX News reference: 8965
ORX Standard: Banking

Published In Media	Occurrence - From	Occurrence - To	Discovery Date	Recognition / Settlement
07 September 2019				

Boundary Risk Other Risk	**Industry Event**	**Scenario** SC0002 - 3rd Party Fraud
Product PD0601 - Consumer Current Accounts	**Process** PC0102 - Product Development	**Event Closed** No
ORX Member Yes	**Role of Firm** LS0307 - Position Taking (Principal)	**Jurisdiction / Choice of Law** LS0105 - Western Europe (excluding United Kingdom)
Cause 1 CS0102 - Assault by Criminals / Terrorists	**Cause 2**	**Cause 3**
Counterparty LS0207 - Individual - Retail	**Environmental Volatility** LS0406 - Not Identifiable	**Provision** No

Source(s)

https://kassa.bnnvara.nl/nieuws/gedupeerden-qr-fraude-krijgen-van-ing-schade-vergoed
https://www.telegraaf.nl/financieel/2098364990/ing-vergoedt-schade-door-truc-met-qr-code
https://radar.avrotros.nl/nieuws/item/ing-vergoedt-schade-van-oplichting-met-qr-codes/
https://kassa.bnnvara.nl/gemist/nieuws/ing-gaat-slachtoffers-qr-fraude-toch-vergoeden

Related links