Hackers have stolen user contact information, including email addresses and phone numbers, from the website of the European Central Bank and attempted to extort money from the institution. The attackers exploited a vulnerability to access a database serving the ECB's public website, the institution announced Thursday on its website . No internal systems or market sensitive data were affected, the ECB said.

The compromised database primarily contained contact information provided by users when registering for various ECB events and conferences. Most of the data was encrypted, but email addresses, phone numbers and street addresses were not, according to the ECB.

The database contained around 20,000 email addresses and a lower number of phone numbers and physical contact addresses, an ECB spokeswoman said Thursday. It's not known at this time if the attackers copied the entire database or only parts of it, but 95 percent of the information in the database was encrypted, she said.

ECB learned of the breach late Monday night when it received an anonymous email from the attackers seeking financial compensation for the data.

The ECB has not and will not pay anything, the ECB spokeswoman said.

The incident was reported to police in Frankfurt, where the ECB is headquartered, and an investigation has been launched. The Frankfurt police did not immediately respond to an inquiry seeking more information about the extortion attempt.

The ECB has reset all user passwords on its website as a precaution and is contacting people whose email addresses and other data might have been compromised. The vulnerability exploited by the attackers has been identified and fixed.

Given that people typically interested in ECB events work in the financial industry, the stolen email addresses could prove a valuable resource for phishers.

The affected individuals could be at a higher risk of fraud and phishing attacks following this security breach, said Jon French, a security analyst at email and Web security firm AppRiver, via email. Personal information about the target could make a phishing attack more convincing than a random spam email. "Likewise the attacker could just attempt to use the gained personal data and attempt to use it to commit fraud."

Extortion attempts using stolen customer data are increasingly common. In June, hackers threatened to release stolen personal information on more than 650,000 French and Belgian customers of Domino's Pizza
unless the company paid them 30,000 euros
(over US$40,000).

"Unless we're missing some important facts, it makes little sense for the ECB to pay a hacker money in this circumstance, as there's no guarantee that he won't also sell access to the data in addition to getting the ransom," said Tim Erlin, director of security and risk at security firm Tripwire, via email. "Data isn't the same as a physical object or person. It's copied, not stolen."

source: IDG News Service