

## WHAT TO DO IN THE EVENT OF A CYBERATTACK ON A CREDIT INFORMATION ORGANIZATION

On 10 September 2025, the Vietnam National Cyber Security Emergency Response Center (VNCERT) confirmed a significant cyberattack targeting the National Credit Information Center of Vietnam (CIC), a unit under the State Bank of Vietnam. The attack involved unauthorized access with the apparent intent to steal personal data.

In response, VNCERT initiated emergency technical and investigative measures in coordination with leading cybersecurity firms, CIC, and relevant authorities from the State Bank. While the full extent of the data breach is still under investigation, precautionary alerts have been issued across the financial sector to mitigate potential risks.

### Why It Matters

According to the Vietnamese data protection regulations, credit information providers such as CIC – under many circumstances – act as **Data Processors**, while banks remain the **Data Controllers**.

This distinction is crucial in breach scenarios:

- Providers must notify their customer banks.
- Banks must conduct a risk assessment and notify competent authorities.
- Depending on the severity and nature of the breach, banks may also need to notify affected individuals.

The result is a multi-layered notification chain, intensifying compliance and operational challenges.

### Recommended Actions for Banks and Financial Institutions

In light of this incident, banks should promptly:

1. **Assess exposure** – Verify whether customer data under their control was implicated.
2. **Coordinate with CIC** – Ensure timely and accurate information-sharing.
3. **Conduct risk assessments** – Evaluate the likelihood and impact of harm to individuals.
4. **Prepare notifications** – Where required, notify the Ministry of Public Security (MPS).
5. **Educate customers** – Warn against possible phishing, fraud, or identity theft attempts leveraging leaked data.

This event underscores the critical importance of breach readiness, vendor oversight, and coordinated incident response in Vietnam's financial sector.

## KPMG is Here to Support

In times of heightened cybersecurity risk, timely and coordinated response is critical. KPMG stands ready to assist banks and financial institutions in:

- Navigating regulatory notification requirements
- Conducting breach impact assessments
- Enhancing cybersecurity posture and vendor oversight
- Strengthening incident response capabilities

Our multidisciplinary team combines deep regulatory knowledge with technical expertise to help you manage risk, maintain trust, and ensure compliance.

Please reach out to your KPMG contact for tailored support and guidance.

## Contact us

Email: [info@kpmg.com.vn](mailto:info@kpmg.com.vn)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG Limited, KPMG Tax and Advisory Limited, KPMG Law Limited, KPMG Services Company Limited, all Vietnamese one member limited liability companies and member firms of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.



Scan to visit our website: [kpmg.com.vn](https://kpmg.com.vn)