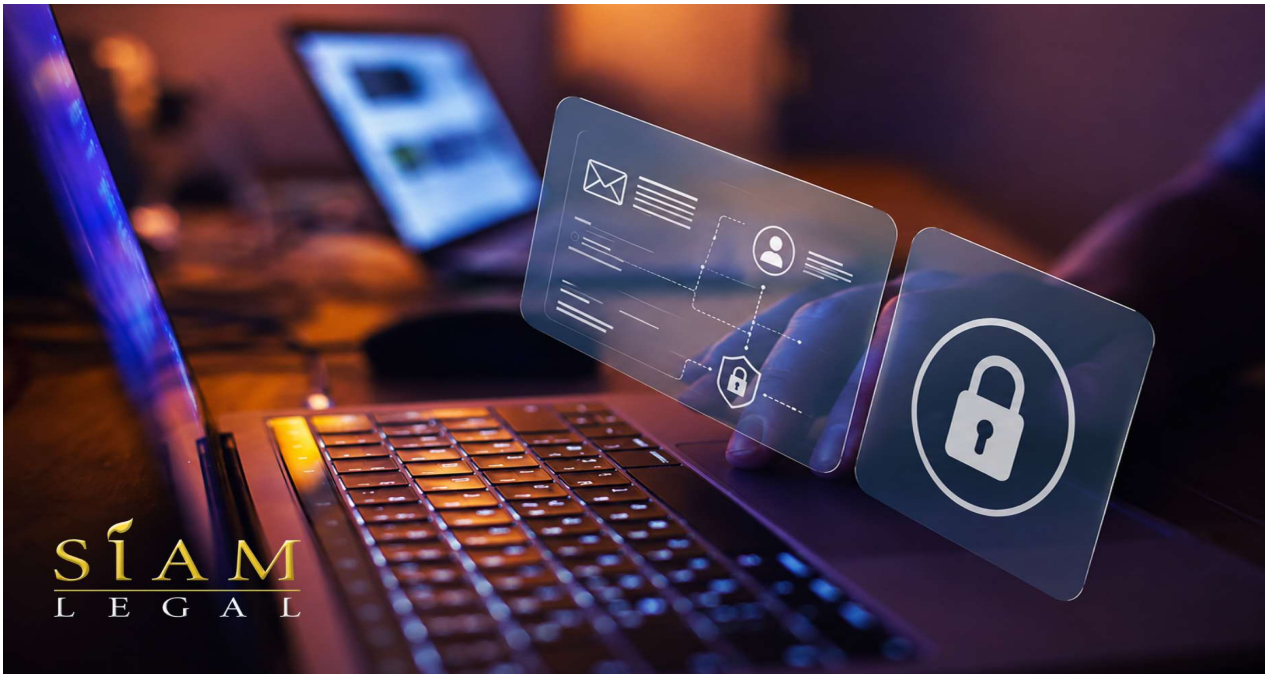

Siam Legal International Advises Thailand Businesses on Legal Risks Following Rise in Executive Email Fraud

June 05, 2026

Bangkok, Thailand - June 05, 2026 - PRESSADVANTAGE -

Siam Legal International is urging businesses in Thailand to strengthen payment verification procedures following recent warnings from the Anti-Cyber Scam Center (ACSC) about fake emails targeting company executives, finance teams, and business partners.

The ACSC reported 5,583 online fraud complaints between May 17 and 23, 2026, with total losses reaching 214.3 million baht during the same period. Although the number of complaints fell slightly compared with the previous week, total damages rose by 12.5 million baht, showing that financial losses from online fraud remain a serious concern for individuals and businesses in Thailand.

Investment scams caused the highest losses during the reporting period, reaching 83.3 million baht. Goods and services fraud remained the most common category, accounting for more than 4,700 cases, or nearly 85% of all complaints. The ACSC also noted a sharp rise in proactive technical cyber-attacks, with cases increasing from 5 to 23 in one week and associated losses rising from 2.2 million baht to 8.4 million baht.

Of particular concern to businesses is the rise of CEO fraud and business email compromise schemes. These attacks involve criminals impersonating senior executives, parent companies, suppliers, or business partners to request urgent transfers, invoice payments, or changes to recipient bank account details. Scammers often use email addresses that closely resemble legitimate company emails, sometimes differing by only a few characters. They may also use company logos, executive names, and familiar business language to make the request appear credible.

?Business email compromise is particularly dangerous because it targets ordinary company workflows, including invoice payments, supplier communications, and executive approvals,? said Kittisak Sriparesri, Attorney at Law at Siam Legal International. ?When a fraudulent transfer occurs, businesses should act quickly to preserve evidence, contact the relevant financial institutions, review internal records, and determine whether formal reporting or legal action is necessary.?

Siam Legal International recommends that companies review their internal payment controls and establish clear procedures for verifying transfer instructions. Businesses should not rely only on email approval for high-value transactions, urgent payment requests, or changes to supplier bank account details. Instead, finance teams should verify such requests through a separate communication channel, such as a direct phone call to a known contact or confirmation through an established internal approval process.

The firm also recommends dual approval requirements for significant transfers, regular staff training on identifying suspicious emails, and documented procedures for reviewing new payment instructions. Employees responsible for finance, procurement, administration, and executive support should be trained to check email domains carefully, identify unusual urgency, and question requests that bypass normal company procedures.

Foreign-owned businesses and companies with international operations may face additional exposure because criminals can exploit time zone differences, cross-border payment flows, language gaps, and communication delays. A fraudulent email that appears to come from a parent company, overseas supplier, or senior executive can pressure local staff into acting quickly before proper verification is completed.

Companies that fall victim to email fraud may face consequences beyond the immediate financial loss. These may include disputes with legitimate suppliers, internal accountability issues, insurance questions, regulatory concerns, and potential liability to shareholders, clients, or business partners. In some cases, businesses may also need to assess whether company systems were compromised or whether the fraud was limited to email impersonation.

Siam Legal International advises companies affected by suspected email fraud to preserve all email records,

payment instructions, bank transfer documents, internal approvals, invoice records, and related communications. Businesses should also contact their financial institution as quickly as possible and consider whether formal reporting or legal action is appropriate under Thailand?s cybercrime, fraud, and related criminal laws.

The firm notes that early action can be important in cybercrime matters, particularly where funds have been transferred to unknown accounts or where company systems may have been compromised. Businesses should also review their internal controls after an incident to reduce the risk of repeat attacks.

Siam Legal International assists businesses, foreign investors, and individuals with legal guidance involving suspected online fraud, digital evidence, financial scams, criminal complaints, and related cybercrime issues in Thailand. Businesses affected by executive email fraud or business email compromise may benefit from speaking with a cybercrime lawyer in Thailand to understand evidence preservation, reporting options, and potential legal remedies.

###

For more information about Siam Legal International, contact the company here:Siam Legal InternationalRex Baay+662 254 8900info@siam-legal.com18th Floor, Unit 1806 Two Pacific Place,142 Sukhumvit Rd, Khlong Toei,Bangkok 10110, Thailand

Siam Legal International

American-managed Thailand law firm with 22+ years? experience. Experts in corporate setup, BOI, FBL, family & divorce, property, litigation, immigration, notary, wills, contracts & due diligence across Bangkok, Phuket, Pattaya & more.

Website: https://www.siam-legal.com/

Email: info@siam-legal.com

Phone: +662 254 8900