



International Trade Administration Commission of South Africa

Private Bag X753, Pretoria, 0001
Thalukanyo Nangammbi, Cell: 082 040 4446
Enquiries: tnangammbi@itac.org.za
URL: <http://www.itac.org.za/>

Press Release
15 April 2024

NOTIFICATION OF A PERSONAL INFORMATION SECURITY COMPROMISE

1. The International Trade Administration Commission of South Africa (“**ITAC**”) in discharging its general functions as outlined in Part B (sections 15 to 22) of the International Trade Administration Act 71 of 2002 (“**the Act**”), handles and processes a diverse set of personal information. We do so with a degree of care to protect your personal information, which is why, as a precautionary measure, we are publishing this notice to let you know about a security compromise that may involve your personal information.
2. The International Trade Administration Commission of South Africa (“**ITAC**”) experienced a security compromise on 2 January 2024. Specifically, ITAC suffered a ransomware attack in which malicious actors encrypted ITAC’s files and locked users out of their systems and demanded a ransom payment in exchange for restoring access or decrypting their files (“**the Security Compromise**”).
3. Please note that the delay in the publication of this notice was due to the need for ITAC to investigate the Security Compromise and restore the integrity of its information systems. Also, it was considered vital not to pre-empt the investigations that had been initiated since ITAC became aware of the Security Compromise.
4. The type of information held on ITAC’s servers includes personal information relating to ITAC’s employees, service providers, importers, exporters and other stakeholders (“**Stakeholders**”).

5. After ITAC's information technology team became aware of the Security Compromise on 2 January 2024, subsequently taking the following steps to contain the Security Compromise:
 - 5.1. We immediately shut down the affected servers and restored backups of the data on the affected servers;
 - 5.2. We upgraded our firewall and antivirus measures to the highest possible security levels;
 - 5.3. We reported the Security Compromise to the relevant authorities for further investigation;
 - 5.4. We appointed a forensic service provider to conduct vulnerability and penetration testing to determine and close the gaps in our systems. The service provider will also undertake a comprehensive forensic investigation, to understand the nature and root cause of the Security Compromise, including the containment and recovery of our systems. The service provider will further assist us in ensuring that the remediation process is completed to prevent the reoccurrence of the Security Compromise; and
6. We will continue to enhance data privacy and protection measures, such as implementing and increasing encryption and multi-factor authentication, and any additional technological measures our forensic service provider recommends, to address new risks to personal information.
7. We assure you that we have taken all the reasonable steps to contain the Security Compromise and to reduce the likelihood of similar incidents occurring in the future. Over and above our ongoing investigation, we have requested our forensic service provider to remedy all weaknesses in our information technology environment.
8. We are therefore publishing this notice to alert all Stakeholders to the fact that there is a chance this Security Compromise may affect them. It is therefore important that you know that the person who perpetrated the Security Compromise may have accessed, and possibly extracted, personal information that you submitted to ITAC.

9. It is important to remember that access to your personal information can create opportunities for your information to be used in unlawful ways. We therefore urge you to be vigilant and to follow these recommendations:
- 9.1. never disclose Personal Identification Numbers (PINs), passwords or One Time Passwords (OTPs) via phone, fax, text messages or email;
 - 9.2. only provide personal information to verifiable sources;
 - 9.3. do not click on suspicious links;
 - 9.4. if you receive unwanted marketing calls, confirm how your details were obtained and ask to be removed from the marketing database; and
 - 9.5. if you have engaged with ITAC recently, treat any communications you may receive from anyone purporting to be from ITAC, with extra vigilance and caution.
10. We value your privacy and deeply regret that this incident has occurred. We are working closely with the Information Regulator South Africa to ensure that the Security Compromise is properly addressed.
11. We sincerely apologise for the Security Compromise. This is not an experience we wish to create for any of our valued Stakeholders.
12. Please contact ITAC's Information Officer on informationofficer@itac.org.za if you have any questions or queries. We would be grateful to receive queries via this email address in order to adequately track and timeously respond to your queries.

Yours Sincerely,

Mr Ayabonga Cawe,

Chief Commissioner and Information Officer,

International Trade Administration Commission of South Africa.

ISSUED BY THE INTERNATIONAL TRADE ADMINISTRATION COMMISSION OF SOUTH AFRICA