Loss Event

Banking

SBM Holdings
EL0201 - External Theft & Fraud
IN - India

BL0401 - Commercial Banking
USD 4,000,000.00 | US Dollar
Asia / Pacific

State Bank of Mauritius' India operations lose up to USD 4 million in cyberattack

On 2 October 2018, State Bank of Mauritius' (SBM) Indian operations fell victim to a cyber fraud potentially resulting in losses of up to USD 4 million (EUR 3.5 million). The attack was first reported by SBM's parent company, SBM Holdings, on 3 October 2018.

In its initial announcement, SBM Holdings said the attack had resulted in a potential loss of USD 14 million and in a subsequent announcement on 4 October 2018, the group said the potential loss had been reduced to USD 4 million. This was as a result of recovery efforts.

SBM Holdings said that the relevant authorities had been informed, that the Indian operations were carrying out a cyber security review and that no customers had experienced losses. It advised shareholders and investors to exercise caution when dealing in the shares of SBM.

According to Business Insider, the attack was coordinated via a breach of the bank's SWIFT money transfer systems. However, as of 4 October 2018, this has neither been confirmed nor have further details on the fraud been disclosed.

Author Andreia Stephenson **Published Date** 04 October 2018 **Last Update** 08 October 2018

Source(s)

Related links

https://www.sbmgroup.mu/newsroom/communique/sbm-holdings-ltd-cautionary-announc…

,

https://www.sbmgroup.mu/newsroom/communique/sbm-holdings-ltd-cautionary-announc…

,

https://www.businessinsider.in/State-Bank-of-Mauritiuss-Indian-branch-just-beca…

,

https://www.business-standard.com/article/companies/state-bank-of-mauritius-ind…

Event

Published In Media	Date of Occurrence - From	Date of Occurrence - To	Discovery Date	Date of Recognition/Settlement
03 October 2018	02 October 2018	02 October 2018		

Loss Amount USD	Loss Amount EURO	Provision	Boundary Risk
4,000,000.00	3,463,520.00	No	Other Risk

Industry Event	Scenario	Product	Process
	SC0024 - Cyber-Related Fraud	PD9900 - Not Product-Related	PC1004 - IT Security

Event Closed	ORX Member	Role of Firm
No	No	LS0307 - Position Taking (Principal)

Cause 1	Cause 2	Cause 3
CS0102 - Assault by Criminals / Terrorists	CS0503 - Software - Inadequate Maintenance	

Jurisdiction / Choice of Law	Counterparty	Environmental Volatility
LS0103 - Rest of the World	LS0212 - Not Identifiable	LS0406 - Not Identifiable