

Fawry announces Conclusion of cybersecurity investigation

26 November 2023 – (Cairo, Egypt) Fawry (the "Company", FWRY.CA on the Egyptian Exchange), Egypt's leading provider of e-payments and digital finance solutions, has now completed a comprehensive investigation and analysis of its cybersecurity infrastructure, following speculation earlier this month about a breach of its systems by ransomware attacker LockBit. Fawry engaged Group-IB, a leading creator of cybersecurity technologies that investigates, prevents, and fights digital crime, to investigate an incident after the ransomware group LockBit published a sample of data on its dedicated leak site on November 8th, which was allegedly stolen during a breach of Fawry's infrastructure.

As of November 24 Group-IB's [Digital Forensics](#) and [Incident Response](#) (DFIR) team has confirmed in its final report that Fawry's production segment, the live environment which hosts the myfawry, banking applications, Acceptance, Retail and Fawry Plus, was out of scope of the LockBit ransomware attack and not subject to a breach. This assessment supports Fawry's initial announcement of November 10 that its live production environment had not been subject to a breach and that no banking and card data have been exfiltrated from the platform.

Group-IB has also confirmed, however, that an isolated part of Fawry's testing environment, which is used to model and trial changes to its platform and is completely isolated from the production environment has been subject to a previous attack. The attack successfully encrypted some files and allegedly exfiltrated data. Fawry remains confident that this data will not impact financial transactions on its platform, but the company believes it may have included the personal details of some customers whose information had been on the testing platform as part of a system migration projects. These details include contact information, such as addresses and phone numbers, in addition to customers' dates of birth. While they do not pose a security risk to financial transactions, the safety of our customers' assets remains our highest priority. If any customer is concerned about their data, advice is available on the Fawry.com website, or by calling the Fawry customer care center.

Group-IB's DFIR team started its incident response engagement on November 9. Over the course of three days they deployed the company's proprietary [advanced monitoring solutions](#) across 100% of Fawry's server infrastructure. Both segments — production and testing environments — are clean as of November 24 of LockBit presence. The Fawry team has performed a 100% incident eradication of observed indicators of LockBit code, and Group-IB experts have confirmed the completion of the network cleanup.

At the time of writing, Group-IB's [advanced monitoring solutions](#) is covering 100% of Fawry's production and testing environments, as confirmed by Fawry's infrastructure team.

In response to the findings, Fawry has notified and is working closely with Egyptian regulators as it seeks to recover the data that may have been stolen.

Fawry Founder and CEO, Ashraf Sabry stated: "We are satisfied that any compromise of Fawry's systems has been neutralised and that the professional investigation we instigated will reassure customers that all financial records and data remain secure on the company's production servers. The safety and security of our customers' assets remain our absolute priority, and we are committed to take all necessary steps to avoid similar incidents in the future".

Press Release

26 November 2023

Group-IB will continue to provide active monitoring of Fawry's systems for the foreseeable future and validate the need for any extra security measures as required.

In addition, Fawry is in active discussions with a range of global consultancy firms to review the group's policies for governance and risk assessment and to advise on the development of existing frameworks to adopt the latest international frameworks.

– Ends –

About Group-IB

Founded in 2003 and headquartered in Singapore, Group-IB is a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime. Combating cybercrime is in the company's DNA, shaping its technological capabilities to defend businesses, citizens, and support law enforcement operations.

In November 2023, Group-IB will celebrate the 20th anniversary of its founding with a range of exciting events marking the company's global growth and significant contribution to international law-enforcement efforts aimed at stamping out cybercrime.

Group-IB's Digital Crime Resistance Centers (DCRCs) are located in the Middle East, Europe, and Asia-Pacific to help critically analyze and promptly mitigate regional and country-specific threats. These mission-critical units help Group-IB strengthen its contribution to global cybercrime prevention and continually expand its threat-hunting capabilities.

Group-IB's decentralized and autonomous operational structure helps it offer tailored, comprehensive support services with a high level of expertise. We map and mitigate adversaries' tactics in each region, delivering customized cybersecurity solutions tailored to risk profiles and requirements of various industries, including retail, healthcare, gaming, financial services, manufacturing, critical services, and more.

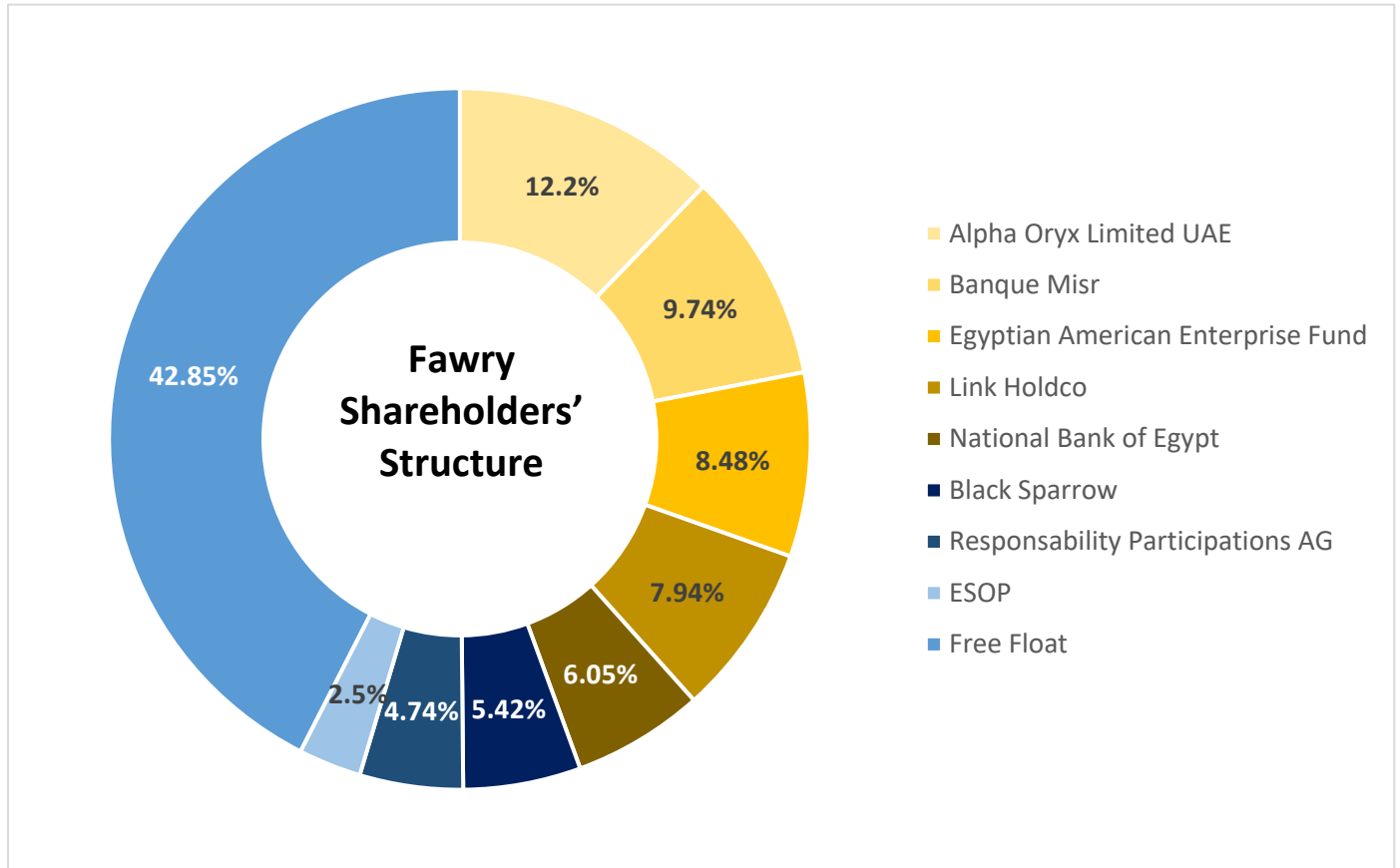
The company's global security leaders work in synergy with some of the industry's most advanced technologies to offer detection and response capabilities that eliminate cyber disruptions agilely.

Group-IB's Unified Risk Platform (URP) underpins its conviction to build a secure and trusted cyber environment by utilizing intelligence-driven technology and agile expertise that completely detects and defends against all nuances of digital crime. The platform proactively protects organizations' critical infrastructure from sophisticated attacks while continuously analyzing potentially dangerous behavior all over their network.

The comprehensive suite includes the world's most trusted Threat Intelligence, The most complete Fraud Protection, AI-powered Digital Risk Protection, Multi-layered protection with Managed Extended Detection and Response (XDR), All-infrastructure Business Email Protection, and External Attack Surface Management.

Furthermore, Group-IB's full-cycle incident response and investigation have consistently elevated industry standards, crafted over 70,000+ of cybersecurity incident response completed by our sector-leading DFIR Laboratory, High-Tech Crime Investigations Department, and round-the-clock CERT-GIB.

About Fawry for Banking Technology and Electronic Payments



Founded in 2008, Fawry is the largest e-payment platform in Egypt serving the banked and unbanked population. Fawry's primary services include enabling electronic bill payments, mobile top-ups and provisions for millions of Egyptian users. Other digital services also include e-ticketing, cable TV, and variety of other services. Through its peer-to-peer model, Fawry is enabling corporates and SMEs to accept electronic payments through a number of platforms including websites, mobile phones, and POSs. With a network of 36 member banks, its mobile platform and 324 thousand agents, Fawry processes more than 4 million transactions per day, serving an estimated customer base of 50 million users monthly. Learn more at www.fawry.com.

Media contact details

Wael Wahby, Hannah Burns and Nigel Fairbrass:

fawry@eternapartners.com