Covid-19 Security Alert From Mastercard

The COVID-19 pandemic has triggered a notable increase in cyber-attacks as fraudsters look to take advantage of system vulnerabilities and changes in the new working environment. These types of attacks can result in significant losses within a short period of time, without the issuer or its processor being aware.

Now, more than ever, it is critical for organizations to remain vigilant and to investigate and mitigate fraudulent activities by taking prompt and appropriate action.

As your trusted partner, we are here to support you.

To stay alert, protected and to mitigate against large-scale fraud, Mastercard recommends that organizations heighten their fraud prevention, monitoring and response operations at this time.

The following three-point protection plan provides a checklist of activities and solutions that can help you achieve this.

Please ensure that your Security Contact information is updated in the Company Contact Manager in Mastercard Connect to adjust for employees that may be working remotely or do not have access to internal emails.

1. Protect your authentication and authorization networks

- **Monitor for unusual traffic** from specific locations, merchants and acquirers – this could be a red flag.
- **Test vulnerabilities** of your host and authorization system for Mastercardbranded cards with threat scanning capabilities, such as Mastercard Threat Scan, to shore up any weak links and secure against attacks.
- **Ensure basic authentication methods** are consistently in place and adopt the latest authentication methods where feasible, ideally a combination of physical and behavioral biometrics, such as Identity Check and NuDetect, to mitigate risk associated with card not present transactions.
- **Deploy spending policy rules** to mirror your authorization strategy, dictating how transactions are authorized for certain markets, channels or transaction types, and layer protection against attacks.
- **Review whitelisted accounts**, particularly accounts that may have been whitelisted for magstripe transactions.
- **Test your connectivity** to the Fraud Center in Mastercard Connect™ to ensure continual support of your day-to-day risk management activities, both in the office and remotely. Ensure remote employees can effectively monitor fraud alerts and declined transactions.

2. Protect your business in cyber environments

- **Be hyper vigilant for phishing emails** as cyber criminals have been exploiting COVID-19 to send malicious emails that purport to come from legitimate sources. Employees should be cautious about clicking on links or attachments in emails. Employers can ensure email authentication schemes are implemented to help prevent email spoofing, a scheme commonly used in phishing attacks.
- **Ensure systems are patched** with the most up-to-date software versions. Cyber actors are constantly scanning the internet for websites using end-of-life or outdated versions of software. By ensuring systems are fully patched, companies can help prevent attackers from exploiting known vulnerabilities.
- **Apply strong passwords and remote connection policies** for all employees, especially those connecting remotely. Access to administration interfaces should be protected with two-factor authentication, such as trusted IP addresses or onetime pass code.
- **Pay attention to new merchant accounts** and have strong KYC (Know Your Customer) procedures in place to ensure you are acquiring for legitimate merchants amidst the recent proliferation of malicious and suspicious coronavirus-related web domains.

3. Protect your consumers' payment journey

- **Scan payment networks** for intrusion and indicators of compromise. Investigate alerts, such as Safety Net alerts and security alerts, promptly and use transaction based decisioning powered by artificial intelligence, such as Decision Intelligence, to help prioritize alert review.
- **Review fraud rules**, ensuring rules for high-risk transactions are set to decline or alert mode and applying diligent monitoring. Examples of high-risk transactions include irregular or higher than usual purchases or cash withdrawals, multiple transactions by the same card, transactions from high-risk locations, and transactions with validation failures.
- **Ensure you have a current Incident Response Plan** to minimize potential financial loss and disruption to normal operations, should an attack take place.

For 24/7 support, contact the Mastercard Cyber & Intelligence team at fraud.support@mastercard.com or on +1-800-999-0363 (inside the U.S.), +1-636-7226176 (outside the U.S.), +32-2-352-54 03 (Europe).

If you are experiencing fraud or a significant event affecting your authorization or clearing processing, call the Mastercard Operation Command Center on +1 636 722 6176.

To learn more about Cyber & Intelligence security tools and solutions, visit Mastercard Connect™ or speak to your Mastercard representative.