MERRILL
A BANK OF AMERICA COMPANY

CYBERSECURITY CHECKLIST

Consider taking these steps if your business has been targeted

Best practices to help your business respond to a cyber event

- ❑ **Prepare and don't delay.** An immediate, strong response always helps to better address any incidents. Understand your cyber insurance policy (if you have one) and follow any guidelines outlined. A planned response to any event is critical to mitigating any risks. Acting quickly after a cyber event can minimize damage to your business.

- ❑ **Detect and assess.** Identify (if possible) what happened, where and when the incident was first reported, and document whether it was successful, including any losses or damage by scanning all company networks to determine the extent of the intrusion or compromise. Work with internal or partner cybersecurity professionals to eradicate any suspicious programs or unauthorized access and set up better defenses before you go back online. Be sure to apply all software patches and security updates.

- ❑ **Report.** Contact your bank and other financial institutions if you believe your accounts have been compromised. Report fraudulent transactions as soon as you can. To protect at-risk corporate assets, ensure access to bank systems have been secured and emergency workflows for any financial activities are followed.

- ❑ **Initiate recovery.** Begin recovery of systems and data to pre-incident status once all evidence of the intrusion has been eradicated. Instruct all affected personnel to reset passwords and systems access controls, preferably while utilizing MFA or similar authentication methods. If you've experienced an incident that has compromised multiple accounts, require your employees to change their passwords to prevent criminal access of key systems and financial data.

See important information on page 2

MERRILL
A BANK OF AMERICA COMPANY

- ❑ **Review and improve your cyber policies.** Take lessons learned from the incident and review and improve cyber policies and response plans. Ensure that your employee training, firewalls, antivirus software and email protection are up to date and take steps to improve the effectiveness of your business network protection. To protect against future financial fraud, require multiple-person approvals for account and financial change requests. Use verified contact information from within the company's internal contact management system when verifying requests to change information or transfer funds.

- ❑ **Document everything about the event.** The more information you have, the better prepared you will be to assist an investigation, and the better prepared you will be against future cybercrime attempts.

- ❑ **Contact law enforcement. Know and follow your local laws and guidelines for cyber incidents.** If you discover evidence that account credentials or data has been stolen, or you experience financial loss, file a report. Companies that do business on a national level should also reach out to the FBI's Internet Crime Complaint Center (www.ic3.gov).

For more tips and insights, visit ml.com/privacy-and-security-center/additional-resources.html

8436710