

## Your business has been struck by a fraud attack. What should you do?

Every day, businesses become victimized by fraudsters. Preparation and response can make a difference on the impact of the event. Here is a sample framework to consider:

### Have a plan in place

Before fraud strikes, it's important to have a response plan in place. That plan will vary by organization, but it should:

- Identify Key Stakeholders
- Define the role of each stakeholder
- Identify event owner
- Create a fraud event playbook

### Engage and respond

Once the fraud event occurs, it's time to activate the response plan:

#### Assess the Fraud Risk

- Is this an active event or has it concluded?
- What is the severity/impact? Use assessment matrix.
- What is the financial exposure?

#### Assemble broader team

- Stop the event – prevent further impact
- Manage event based on complexity and severity

#### Engage external resources where appropriate

- Financial Institution
- Forensic Accountant, Security Expert
- Law Enforcement
- Vendor

When you have returned to normal operations it's time to review and evaluate

### Investigate

- Assess causes and failure points
- Identify key findings
- Evaluate options and solutions

### Improve Controls

- Develop action plan for key findings
- Implement additional tactical and structural control
- Update internal controls
- Apply learnings through education
- Conduct fraud risk assessments
- Update fraud event management plan

### Key Stakeholders

Senior Management	Information Technology	Risk Management
Business Controls	Media Relations	Treasury/ Finance
Legal	Internal Audit	Other Staff

### Assessment Matrix

		Impact				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Medium	High	High	Extreme	Extreme
	Likely	Medium	Medium	High	High	Extreme
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	Medium

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations.  
 General [disclaimer](#) for Bank of America Merrill Lynch. ©2018 Bank of America Corporation. ARHSSYQC