

# CAPP

## Cyber Attack against Payment Processes Exercise



### *New Scenarios and Exercise*

***What would your financial institution do in the event of a cyber attack on your online banking environment?***

What about an attack on your corporate customers? Your ACH processing systems? Website? Wire process? Debit cards? What would it take to get your processes back to normal?

Over a three day period this fall, in conjunction with FS-ISAC, the Payments Risk Council is conducting a simulated attack on payment processes to help you gauge your financial institution's readiness in the event of such an attack or event.

A similar exercise was conducted in November 2011 that helped the industry identify ways to prevent, detect and respond to cyber attacks against payment processes. In a time when account takeover, breaches at technology companies, denial of service attacks and other cyber-crimes are affecting the industry, it is imperative that your financial institution knows how to react if it happens to you.

Your organization can't afford to miss the 2012 CAPP Exercise.

### **Benefits**

***By participating in this simulated cyber attack exercise, your organization will be able to....***

- Evaluate your current risk mitigation procedures related to cyber attacks and identify potential critical gaps in planning.
- Engage in a live test of your incident response team's ability to respond to major incidents.
- Raise awareness and educate your staff regarding procedures to respond to complex threats.
- Benchmark your business practices based on other Financial Institution responses.
- Develop appropriate risk mitigation recommendations in response to the types of attacks used in this exercise.
- Receive an after-action report highlighting lessons learned from the exercise and category benchmark results.
- Demonstrate regulatory compliance.

**Register Now - [www.fsisac.com/capp](http://www.fsisac.com/capp)  
Earn up to 3.6 AAP Credits**



# CAPP

## Cyber Attack against Payment Processes Exercise

*Choose from two weeks*

November 7-9, 2012

or

November 13-15, 2012

[www.fsisac.com/capp](http://www.fsisac.com/capp)



## Frequently Asked Questions

### When will this take place?

*Choose from two weeks*

November 7-9, 2012 *Registration Deadline: 11/05/12*

November 13-15, 2012 *Registration Deadline: 11/09/12*

### Who should participate?

*Any financial institution that sends or receives ACH transactions, checks or wires. Any financial institution that utilizes online banking for their customers or members. Any bank or credit union that issues check cards.*

### How much will this cost?

*Participation is free.*

### How much time will this take to complete?

*The exercise will be conducted over three consecutive days and the concluding survey will require less than one hour each day to complete. You will receive each day's scenario in the morning and we ask that you complete the survey portion by 12:00 midnight EST. Organizations may wish to use this as an opportunity to conduct a drill within their own company. Time requirements will vary.*

### What do I get out of participating?

*You will better understand your institution's readiness if faced with a cyber-attack, cyber-crime or other incident that may disrupt your business process. All participants will receive a summary of the exercise results. (Distribution of the results will be made in the first quarter of 2013.)*

### What is FS-ISAC?

*Financial Services Information Sharing and Analysis Center. Launched in 1999, FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. That directive – later updated by 2003's Homeland Security Presidential Directive 7 – mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.*

### What is the Payments Risk Council?

*The Payment Risk Council's goal is to share payment risk information for ACH, checks and wire payments as well as best practices to mitigate payment risk. PRC members are financial institution risk professionals, NACHA risk staff and ACH regional payment association managers.*

### Will this be an actual vulnerability test of my system?

*No, this exercise is only a simulation. Each day of the exercise you will receive an e-mail with that day's scenario, a link to a broadcast of information about the scenarios and a series of questions for your organization to answer. When you are ready to answer the questions, you can click on the link to the survey tool to answer the questions for that day.*

### Will my organization's information be published?

*No, all participants and their input will be anonymous.*

### If my organization is not a member of FS-ISAC, can we participate?

*Yes, this exercise is for the benefit of all organizations involved with payments.*

### Will the exercise require any special software?

*No, you will only need an internet connection and e-mail. You will be provided a link to an on-line survey tool called Survey Monkey where you will enter your responses.*

### What type of job functions should participate in the exercise?

*Payment Product and Operations Managers, Check Card Operations, RDC Operations, Fraud and Risk Managers, Corporate Communications, Legal and Compliance, Call Center Management, IT Security, Treasury Management*

### What will my organization have access to when the exercise is completed?

*You will have peer data to compare through an interactive after-action report. Again, all company information will be kept confidential.*

### How can I use the results to benchmark my own organization's performance?

*Data will be available to you to sort by industry type, geographical location or size.*

