FIS™ Data Restore, A Sheltered Harbor® Solution

Improve Your Cyber Defenses

Today's cyber adversaries aim not only to steal data for financial gain, but also to destroy data to inflict economic harm against an institution, industry or country. If any financial institution or group of financial institutions were to experience a major data destruction event, there could be potential for systemic panic affecting the entire financial system. The Sheltered Harbor® initiative is designed to prevent this from happening by ensuring that critical deposit and brokerage records are stored in a manner that is not susceptible to a cyber-attack and that services would be available even if the institution were compromised.

FIS™ is proud to be a participant in the Sheltered Harbor project and encourages our clients to join as well.

Find out more

What is Sheltered Harbor?

Sheltered Harbor is a financial services' industry initiative led by clearing houses, financial institutions, core processors and industry associations to ensure that critical customer and account records can survive a cyber data destruction attack through the deployment of offline immutable standardized encrypted backups with a recovery framework across the financial industry.

How does it work?

Each night at the close of business, a record is created for each account holder, including their balance and customer information. The record is validated, encrypted, and then sent to an offline data vault to protect the records from a cyber event. Records are kept for one media cycle and then deleted. They would only be used during a declared Sheltered Harbor event.

If FIS processes my data, how do I join Sheltered Harbor?

To join Sheltered Harbor, visit **shelteredharbor.org/join**. To fund this effort, Sheltered Harbor charges participant fees based on a bank's number of accounts and total deposits. FIS will create the Sheltered Harbor files for service bureau institutions who join Sheltered Harbor and subscribe, and pay, for this new FIS service. Sheltered Harbor is much more than technology. By joining, you will become part of a community of your peers focused on ensuring enhanced disaster recovery. This cooperative model will allow rapid restoration of your customer's account data after a significant cyber event. You will be able to tell your regulators, and eventually your customers, that you are participating with other banks and brokerages in a collaborative effort to protect their data.

This will enhance both your institution's and the industry's reputation as it showcases your commitment to your customer's account integrity.
This will enhance both your institution's and the industry's reputation as it showcases your commitment to your customer's account integrity.

If I run FIS or non-FIS software at an in-house location, do I need to join Sheltered Harbor?

Yes, by joining the Sheltered Harbor community, you would be provided the specifications for the Sheltered Harbor environment and become part of the cooperative model for protection against a significant cyber event. Once you join Sheltered Harbor, you could either construct your own Sheltered Harbor vault, or send you records to FIS' Sheltered Harbor vault. By leveraging the FIS vault, you would provide FIS your nightly Sheltered Harbor files to be secured in the FIS Sheltered Harbor vault. This approach provides better risk distribution and a lower cost of development. Once your records are secured, you can notify your regulator that you have implemented protections against a cyber data destruction event.

Find out more

If FIS processes my data, what happens if I don't join Sheltered Harbor?

If you elect not to join Sheltered Harbor, you will not be able to communicate to your regulator that you are Sheltered Harbor ready and you will not be able to participate in Disaster Recovery testing of the Sheltered Harbor files. Sheltered Harbor recovery testing will only be available to Sheltered Harbor members.

What happens if FIS suffers a cyber data destruction event?

FIS has a robust state-of-the-art framework to protect clients from a cyber data destruction event. In the highly unlikely scenario that FIS were to suffer a data destruction event, the Sheltered Harbor data could be used by FIS to assist in the restoration process or be provided back to Sheltered Harbor members for external processing.

Product offerings

FIS is currently developing several product offerings for Sheltered Harbor members. A description is as follows:

Testing the Sheltered Harbor Vault

Overview: Appendix J of the FFIEC Business Continuity Handbook notes that a financial institution should develop plausible threat scenarios to test with their critical service provider. Among these scenarios to consider is a cyber event, including data corruption. Furthermore, the handbook recommends the consideration of an "air gap" to protect against data destruction and corruption. To help fulfill these requirements, FIS will offer testing to Sheltered Harbor members whereby they will be able to validate recovered Sheltered Harbor files to demonstrate both an air gap capability and help satisfy recovery testing from a cyber destruction or corruption event. This service will be offered to Sheltered Harbor members after FIS has deployed the environment for all hosted FIS data center clients.

Third-party Hosting

Overview: FIS is deploying Sheltered Harbor for all FIS-hosted data center Core Platform customers.

FIS software customers not at an FIS data center: If you run FIS software in-house, FIS can provide the programming to create the extract (version pending) and send the data to our FIS vault. This leveraged approach offers air gap protection at a lower cost than developing an onsite vault to the Sheltered Harbor spec.

Non-FIS software customers: If you run non-FIS software but want to leverage the FIS vault, you would provide FIS your nightly Sheltered Harbor files to be secured in the FIS Sheltered Harbor vault. This approach provides better risk distribution and a lower cost of development.

Recovery Service

Overview: Sheltered Harbor is about more than just protection of the data. The Sheltered Harbor organization is developing a recovery spec to outline what a recovery from a Sheltered Harbor event would entail. The objective is to provide critical deposit services within hours of a major event utilizing the Sheltered Harbor data files. This would provide customers with the confidence that they can continue critical activities such as making a deposit, viewing balances, withdrawing funds, using the ATM/Debit networks, or being able to continue to receive or disburse ACH transactions from the deposit account.

The service would help serve as a bridge to provide time for the institution to recover to normal processing. While this is a service no financial institution would ever want to use, it may make the difference in surviving a major cyber-attack.

FIS is currently working on the recovery specification with Sheltered Harbor and various banking agencies and plans to finalize an approach for a recovery service for both hosted and in-house clients once the spec is finalized and released.

Learn more: **cpo.mailbox.client@fisglobal.com**

Have questions?

For additional questions or comments, please contact the FIS Continuity Program Office (CPO) at: **cpo.mailbox.client@fisglobal.com**.

©2018 FIS and/or its subsidiaries. All Rights Reserved.