Global Partner Management Notice

Subject: Discover Data Security Alert – Hospitality Point-of-Sale Breaches

Dated: June 12, 2009

Announcement:
Hospitality Point-of-Sale Environment Breaches
Discover Network is currently investigating multiple cardholder data security breaches targeting the hospitality industry. It is highly recommended that merchants in the hospitality industry review the security of their payment environment with specific attention to passwords and remote access to these environments.

The results of recent forensic investigations revealed that merchant use of default/weak passwords in conjunction with remote access have been a significant contributing factor in these data breaches. Merchants should work with their Information Technology (IT) staff and/or payment system service providers to verify that remote access to the payment environment is configured in a secure manner in accordance with PCI Data Security Standard guidelines including password complexity requirements.

Hackers targeting the hospitality payment environments have installed a number of notable malicious executables on the point-of-sale servers and terminals with the purpose of scanning for additional networked systems, searching for non-compliant storage of track data, setting up services that parse volatile memory for track data, and installing backdoors.

Recommendations
To reduce the risk of a data breach, Discover Network encourages merchants to review their payment environments and include the following best practices:

- Use complex passwords for all access in the payment environment including point-of-sale accounts and remote access.
- Ensure firewall ingress and egress rules limit access to only ports and services that are needed for the environment.
- Install and keep anti-virus and anti-spyware software up to date on all systems. Regularly run and review results of scans for malicious software.
- Reboot point-of-sale systems periodically to clear volatile memory, and consider using a secure file wiping utility that can securely clear the contents of the page (swap) file.

If you detect or suspect a security breach, promptly contact your Acquirer. You may contact Discover Network Data Security at (800) 347-3083 to report a breach. For more information on how to handle a data security breach, visit the Discover Network Data Security Breach page at: DiscoverNetwork.com/databreach

Malicious / Suspicious Files
The following list provides the file names and sizes of malicious software found during previous investigations. Please note that attackers may alter names, sizes, and signatures to avert detection.

Name	Size (Bytes)	MD5
rdasrv.exe	115,000	D9A3FB2BFAC89FEA2772C7A73A8422F2
compenum.exe	54,272	BCC61BDF1A2F4CE0F17407A72BA65413
		C5C3341FBDD38C041E550D5DFF187A8F
csrsvc.exe	75,264 - 76,800	78188F70A8CFE2D0EC239860F6059B41
		63E9791D96996DA6A9D2B43034CD5677
		A3090FBFB7F5708F669B43ED3DB9B3A2
		1F9D0D200321AD6577554CC1D0BB6B69
		EBDE11C2159D4FAD7F8886EEFFA49512
		1F9D0D200321AD6577554CC1D0BB6B69
		93E247C4556EAFCEEBB7FEE7E4F35FE4
dirfilemon.exe	1,161,256 – 1,162,093	B6758B2EAE755AC94C8A9E3C986FE1FD
		F96193C10BFC9ABC6FA99ECE0F72991E
dirmon.chm	Variable	AC15D275D4D01C453AAB907DA7051F81
dnsmgr.exe	1,162,117 – 1,162,134	3004CE6CB7C44605CDF971B74DB3A079
		BF27E87187C045E402731CDAA8A62861
		5036F44472070E7A87DE0370DF9BB756
far.exe	586,752 – 620,032	EE7D411F47B13FB204A188FC37E7FC61
		D1D9C26A77BEB82B13C82E854042DC92
install.bat	43	A7C24031CAE3F29EC0C30D220C52A087
lanst.exe	1,497,345 – 1,528,864	E474D38265517B0A3382504B1008FDFB
		D770ADBEE04D14D6AA2F188247AF16D0
		530D02A3C2022BB17324F2D10C933F10
		166C9A5DD22A817247AB732CA63BC680
		A63D6203D1D7568868EBE7521406B057
mdirmon.exe	1,161,103 - 1,162,194	FB9F8F1BEE8B3FB47D7D84BB2286801D
		291E80AE43172873F01F9CA426828217
memPDumper.exe	75,776	7023239806B5840B4391BCB531CDEAD
		BAAB511F2210228E41C3FFDBE5D3FCE
Name	**Size (Bytes)**	**MD5**
netshares.exe	86,016	ada4be9ab674ef75f4fe8f4317859f21
parser.exe	1,496,837 – 1,496,848	a3280b72080ebcfc2cb6b6fa66706df9
		739dee364f220bfa7e600a81f5f9c916
play.bat	79	FCB37DE3B9B1C831A52A836B7A2F2695
psexec.exe	135,168	579B43E13294EB85FAA7C28B470B19C1
RamDDumper.exe	197,120	3DD47D9EAD4DAD89B0B30423E6AD9E70
		561D8CBD96C903F82B03D7936031BFC5
shareenum.exe	53,248	3ca6ec07c6b840e7a256d09839ba0c4f
WinMgmt.exe	66,048	3e19ef9c9a217d242787a896cc4a5b03

Source: *Discover Data Security Alert, June 9, 2009*

Best Regards,

Global Partner Management Team
First Data Corporation
Email: *Gpm@firstdata.com*

© 2009 First Data Corporation. All Rights Reserved. All trademarks, service marks and trade names referenced in this material are the property of their respective owners. The information contained herein is provided as a courtesy and is for general informational purposes only. This Alert is not intended to be a complete description of all applicable policies and procedures. The matters referenced are subject to change. Individual circumstances may vary. This Alert may include, among other things, a compilation of documents received from third parties. It should not be used as a substitute for reference to, as applicable, association releases, bulletins, regulations, rules and other official documents. First Data shall not be responsible for any inaccurate or incomplete information. This Alert may not be copied, reproduced or distributed in any manner whatsoever without the express written consent of First Data Corporation.