Confirmation.

Electronic Confirmation Security Assessment

		Required for		Reviewed, Appropriate and In Place			
		In-Network	Out-of-Network	Yes	No	Notes	Reviewer
1. SAS 70 Type II							
1.01	Performed every 6 months	√	√				
1.02	Controls for Organization & Administration	√	√				
1.03	Controls for Systems Development & Change Management	√	√				
1.04	Controls for Computer Operations	√	√				
1.05	Controls for Physical Access & Environmental Controls	√	√				
1.06	Controls for Authenticated Proper Source	√	N/A				
1.07	Controls for Authorized Users	√	N/A				
1.08	Controls for Proper Client Authorization	√	√				
1.09	Controls for Data Integrity & System Transmission Integrity	√	√				
1.10	Controls for Electronic Signatures	√	√				
1.11	Controls for Backup & Recovery/Data Retention	√	√				
2. SysTrust Certification							
2.01	Performed every 6 months	√	√				
2.02	Includes Principle of Availability	√	√				
2.03	Includes Principle of Confidentiality	√	√				
2.04	Includes Principle of Processing Integrity	√	√				
2.05	Includes Principle of Security	√	√				
2.06	Includes Principle of Privacy	√	√				
3. Privacy Policy							
3.01	Certified by recognized 3rd party (e.g. TRUSTe)	√	√				
3.02	Includes EU Safe Harbor Certification (highest available)	√	√				
4. Website Authentication							
4.01	Extended Validation SSL Certification by recognized 3rd party (e.g. VeriSign)	√	√				
5. Disaster Recovery Plan							
5.01	Tested at least quarterly	√	√				
6. Hosting Facilities							
6.01	Primary hosting facility with SAS 70 Type II or ISO Certification, minimum tier 4 facility	√	√				
6.02	Separate backup hosting facility with SAS 70 Type II or ISO Certification, minimum tier 4 facility	√	√				

		Required for		Reviewed, Appropriate and In Place			
		In-Network	Out-of-Network	Yes	No	Notes	Reviewer
7. Insurances							
7.01	Rating A+ or better in the current Best's Insurance Reports published by A. M. Best Company	√	√				
7.02	E-commerce Technology Liability	√	√				
7.03	User Privacy Protection to cover 1 year worth of Consumer Credit Monitoring in the event of a security breach	√	√				
7.04	Commercial General Liability	√	√				
7.05	Professional Practice	√	√				
7.06	Umbrella Coverage	√	√				
8. Security							
8.01	Compliant with ISO 27001 Control Objectives	√	√				
8.02	All IT infrastructure & access limited to only company employees (e.g. including System Administration/Root Access)	√	√				
8.03	Physical and logical access control is a managed process (e.g. access control lists, change management, monitoring & logging)	√	√				
8.04	Only dedicated servers are utilized (e.g. no shared computing environments)	√	√				
8.05	All company employees have Federal & State background checks, annual drug testing, and are fingerprinted	√	√				
8.06	Sensitive confirmation data stored using cryptographic algorithms minimum key length 192-bit (e.g. Triple DES)	√	√				
8.07	Confirmation data is transmitted with a minimum of 128-bit SSL using recognized 3rd party encryption certificate (e.g. Verisign)	√	√				
8.08	Intrusion Presentation System (IPS) and Intrusion Detection System (IDS) are both deployed for security	√	√				
8.09	Web application firewall for HTTPS traffic inspection	√	√				
8.10	Defense in Depth strategy deployed	√	√				
8.11	External Vulnerability & Penetration Testing performed by recognized 3rd party (e.g. McAfee Secure)	√	√				
8.12	Internal Vulnerability & Penetration Testing performed using industry standard tools (e.g. AppScan, Webinspect)	√	√				
8.13	Virus protection runs on all servers	√	√				

		Required for		Reviewed, Appropriate and In Place			
		In-Network	Out-of-Network	Yes	No	Notes	Reviewer
9. Electronic Confirmation Process							
9.01	A user cannot electronically sign someone else's name on the confirmation	√	√				
9.02	User activity is logged	√	√				
10. Additional Items							
10.01	Defined Service Level Agreement with Escalation Procedures	√	√				
10.02	Review Service Agreement	√	√				
10.03	Review Privacy Policy	√	√				