Confirmation.

Privacy and Security

Overview

July 2009

Table of Contents

Capital Confirmation Privacy and Security Overview

Patent Information

Capital Confirmation, Inc. has a patent on its business process, U.S. Patent No. 7383232.

SAS 70 Type II Report

Capital Confirmation has SAS 70 Type II performed every 6 months. To view the latest SAS 70 Type II service auditor's report please contact Capital Confirmation's Customer Support at 1-888-716-3577 to request a Non-Disclosure Agreement.

SysTrust Certification

Capital Confirmation has a SysTrust Certification performed every six months and has earned the Seal of Assurance for all five of the SysTrust Service Principles: Availability; Confidentiality; Processing Integrity; Security; and Privacy. To view the latest SysTrust Certification report, please click on the SysTrust Logo on the www.confirmation.com homepage.

Privacy Policy

TRUSTe

Capital Confirmation adheres to the Internet's most trusted third-party privacy policy standards issued by TRUSTe. TRUSTe performs an annual review of Capital Confirmation's site and privacy policy. Here is information regarding TRUSTe's Privacy Seal from the TRUSTe website:

> The TRUSTe Web Privacy Seal empowers customers with confidence. The seal marks companies that adhere to TRUSTe's strict privacy principles, and who strive to treat customer information with the utmost respect.
>
> **TRUSTe Program Features:**
>
> - TRUSTe certifies nearly half of the top 50 U.S. Web sites.
> - TRUSTe resolves 100% of privacy complaints filed by sealholders' customers every year.
> - Provides privacy best-practices in an ever-evolving space.

For more information on TRUSTe please visit www.truste.com.

View Capital Confirmation's TRUSTe Web Privacy Seal certification:
http://www.truste.org/ivalidate.php?url=www.confirmation.com&sealid=101&lang=en

EU Safe Harbor Certification

CCI is EU Safe Harbor Certified by TRUSTe. With the EU Safe Harbor Seal, companies can conduct overseas business in alignment with the safe harbor, a framework created by the U.S. Department of Commerce and European parties to avoid trade disruptions resulting from international privacy laws. Here is information on the Safe Harbor seal from the TRUSTe website:

> The Safe Harbor seal program provides:
>
> - **Web Site Privacy Certification and Oversight**
>
> TRUSTe® certifies the data gathering and dissemination practices of Web sites doing business with European citizens, as well as enforces privacy policies through ongoing monitoring.
>
> - **Online and Offline Dispute Resolution**
>
> EU Safe Harbor requirements for both web-based and offline privacy-related disputes are satisfied through the TRUSTe Watchdog program.

For more information on TRUSTe please visit www.truste.com.

View Capital Confirmation's TRUSTe EU Safe Harbor certification:
http://www.truste.org/ivalidate.php?url=www.confirmation.com&sealid=102

Identity Certification

CCI is identity certified by VeriSign's highest identity certification – the Class 3 Extended Validation SSL SGA CA. Here is the information on the Extended Validation SSL from VeriSign:

> In 2006, a group of leading SSL Certificate Authorities (CAs) and browser vendors approved standard practices for certificate validation and display called the Extended Validation Standard. To issue an SSL Certificate that complies with the standard, a CA must adopt the extended certificate validation practice and pass a Webtrust audit. The validation process requires the CA to authenticate the certificate applicant's domain ownership and organizational identity, as well as the individual approver's employment with the applicant, and authority to obtain the Extended Validation SSL Certificate. VeriSign's Certification Practice Statement outlines their authentication and verification processes.
>
> Extended Validation SSL Certificates give high-security Web browsers information to clearly identify a Web site's organizational identity. For example, if you use Microsoft® Internet Explorer 7 to go to a Web site secured with an SSL Certificate that meets the Extended Validation Standard, IE7 will cause the URL address bar to turn green. A display next to the green bar will toggle between the organization name listed in the

certificate and the Certificate Authority (VeriSign, for example). Firefox 3 also supports Extended Validation SSL. Other browsers are expected to offer Extended Validation visibility in upcoming releases. Older browsers will display Extended Validation SSL Certificates with the same security symbols as existing SSL Certificates.

Web browsers that were developed to recognize EV SSL Certificates are considered high-security browsers. They are designed to trigger unique visual cues to indicate the presence of an EV SSL Certificate. For instance, Internet Explorer 7 shows a green address bar and displays the name of the organization listed in the certificate as well as the certificate's security vendor. These displays make it easier for Web site visitors to quickly establish trust with the Web sites they visit. Microsoft® Internet Explorer 7 and Firefox 3 are examples of high-security browsers.

For more information please visit www.verisign.com.

View Capital Confirmation's VeriSign SSL and Identity Certification:
https://seal.verisign.com/splash?form_file=fdf/splash.fdf&dn=WWW.CONFIRMATION.COM&lang=en

Internet Communications Encryption

CCI uses 128-bit SSL Extended Validation Certificates with Server Gated Cryptography by VeriSign for Internet communications. Here is information on VeriSign's SSL encryption from their website:

VeriSign is the most trusted mark on the Internet

- The world's 40 largest banks and over 95% of Fortune 500 companies choose VeriSign* SSL Certificates.
- VeriSign secures more than one million Web servers worldwide, more than any other Certificate Authority.
- Over 75% of Web sites using Extended Validation SSL choose VeriSign, including biggest names in e-commerce and banking.
- Over 90,000 domains in 145 countries display the VeriSign Secured® Seal, the most recognized trust mark on the Internet.

VeriSign offers the strongest SSL encryption

- High-level encryption, at 128 bits, can calculate 2^{88} times as many combinations as 40-bit encryption. That's over a trillion times a trillion times stronger.
- Only True 128-bit SSL Certificates with Server Gated Cryptography (SGC) enable every site visitor to experience the strongest SSL encryption available to them.
- VeriSign is the leading SSL provider of SGC-enabled SSL Certificates, enabling 128- or 256-bit encryption for over 99.9% of Internet users.

For more information please visit www.verisign.com.

View Capital Confirmation's VeriSign SSL and Identity Certification:
https://seal.verisign.com/splash?form_file=fdf/splash.fdf&dn=WWW.CONFIRMATION.COM&lang=en

Data Encryption

All data deemed sensitive residing within the Confirmation.com system is encrypted. The encryption algorithm is Triple DES and uses three 64 bit keys for a key length of 192 bits. (Effective key length of 168 bits due to parity bits in each 64 bit key.)

Hosting Facilities

Capital Confirmation utilizes Terremark for all of its hosting needs.

Primary Hosting Facility

Terremark has its own SAS 70 Type II and Capital Confirmation's primary hosting facility is located in Terremark's $300 million hosting facility in Miami, Florida. With fortress-style facilities that sit on top of Tier 1 networks from more than 160 global network carriers, Terremark's state-of-the-art Internet Exchange datacenters are unrivaled. Their datacenters provide the right physical security for sensitive business-critical applications including an n+2 redundant power and cooling architecture backed by 100% SLAs. Terremark provides monitoring and on-site technical support 24 hours a day, 7 days a week, 365 days a year. Here is information on the Miami facility – the NAP of the Americas - from Terremark's website:

> Terremark's flagship facility, the NAP of the Americas®, is one of the most significant telecommunications projects in the world. The Tier-IV facility was the first purpose-built, carrier-neutral Network Access Point and is the only facility of its kind specifically designed to link Latin America with the rest of the world.
>
> Miami has been ranked as one of the top-five best interconnected cities in the world, ahead of San Francisco, Chicago and Washington, D.C. Terremark's NAP of the Americas makes Miami the only city in the U.S. where Optical, Ethernet, MPLS, Voice and Internet traffic is handed off in a single location. The NAP of the Americas is located in downtown Miami, an area that has numerous telecommunications carrier facilities, fiber loops, international cable landings and multiple power grids. The convergence of telecommunications infrastructure is why global carriers, ISPs and other Internet-related businesses, educational institutions, and enterprises have chosen to become Terremark clients.
>
> Switching the majority of South America, Central America and the Caribbean's layer-1, layer-2 and layer-3 traffic bound to more than 148 countries in the world, makes the NAP of the Americas the unrivaled gateway to the Americas.
>
> This unique facility provides you with a secure, reliable carrier-neutral facility with direct backbone access to the world's major carriers. Via this massive connectivity, we can deliver to millions of businesses and consumers virtually anywhere in the world any available service from any network service provider in the world.

Building Features:

- 750,000 square foot, purpose-built datacenter
- Tier IV facility with N+2 power and cooling infrastructure
- Equipment floors 32 feet above sea level
- Roof slope designed to aid in drainage of floodwater in excess of 100-year storm intensity assisted by 18 rooftop drains
- Designed to withstand a Category 5 hurricane with approximately 19 million pounds of concrete roof ballast
- 7 inch thick steel reinforced concrete exterior panels
- The building is outside FEMA 500-year designated flood zone

Physical Security

The NAP of the Americas has a centrally-located Command Center manned by security personnel 24 hours a day, 7 days a week, 365 days a year. Security personnel monitor all security cameras, guard building entrance and exit access points, and control key card access to elevators, floors and roof areas. In addition, environmental sensors notify tenants and mobilize rescue in case of emergency.

Backup Hosting Facility

Capital Confirmation maintains a warm backup site at Terremark's Culpepper, Virginia facility. Here is information on the Culpepper hosting facility from Terremark's website:

> Strategically located in Culpeper, Virginia, 60 miles from Washington, DC, the NAP of the Capital Region is the most secure and technologically sophisticated datacenter on the Eastern seaboard.
>
> The 30-acre, multi-datacenter campus is the ideal location for government, enterprise and Web 2.0 clients requiring co-location solutions engineered to meet the needs of today's power, space and bandwidth-intensive mission-critical applications or hot/warm sites for disaster recovery/COOP environments.
>
> The NAP of the Capital Region campus consists of five 50,000-foot independent datacenter structures and one 72,000-square-foot secure office building. Each structure is a secure bunker, designed to provide clients who require it co-location space that meets standards for sensitive compartmented information facilities (SCIFs) managed by Terremark's Federal Group. Inside each datacenter, a professional security staff

maintains and operates sophisticated surveillance systems, biometric scanners and secured areas for processing of staff, customers and visitors.

A complete suite of services from co-location and connectivity to managed hosting and comprehensive disaster recovery solutions is offered, including solutions utilizing Terremark's Infinistructure utility computing platform. Built to 160 watts per square foot, the NAP of the Capital Region easily accommodates today's power requirements for high density computing environments.

Building Features:

- Specifically designed and built as a carrier-grade Federal data communications and hosting facility offering the ultimate in physical security
- 10 ft. earth berm surrounding the entire campus with 150 ft. building set backs
- Compliant fencing, video monitoring, and electronic passage technology
- Roving perimeter security guards and operating building security guards
- DoD-trained anti-terrorism personnel on staff
- Rapid Response Security Force
- Tiered Access Control Protocols compliant and flexible to conform to all levels of established threat conditions
- Primary entrance processing point outside the protected berm
- Isolated shipping/receiving and freight inspection facility (X-ray, etc.)
- No vehicle traffic in the vicinity of data operating buildings
- Parking for 250 vehicles in three (3) separate areas allows for segregation and isolation

For more information on Terremark and its hosting facilities, please visit www.terremark.com.

PCI Compliance

Capital Confirmation maintains PCI compliance through McAfee PCI Compliance certification. McAfee PCI Compliance serves over 250,000 merchants worldwide and meets the requirements of Visa's CISP and AIS, MasterCard's SDP, American Express' DSS, DiscoverCard and JCB. Here is information on McAfee's certification program from their website:

> **Certification of Compliance**
> Separate and distinct from the mandate to comply with the PCI Data Security Standard is the certification, or validation, of compliance whereby entities verify and demonstrate their compliance status. It is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained.

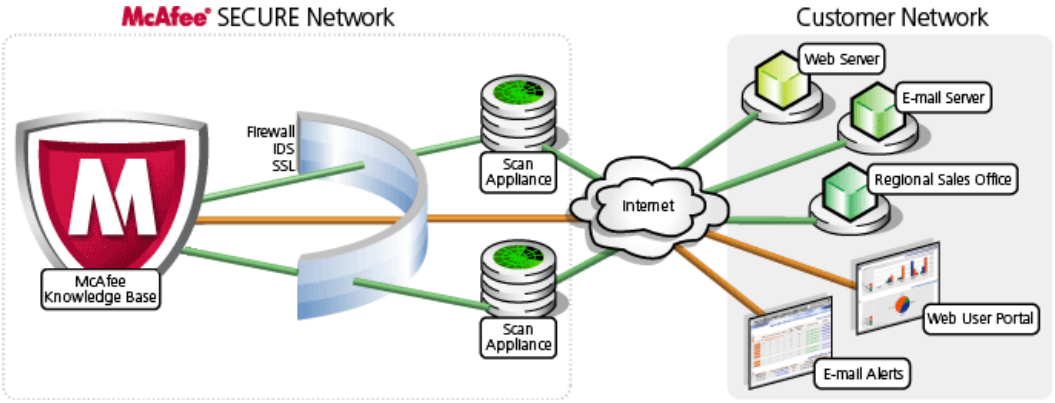
For more information on the PCI Data Security Standard, please visit the PCI Security Standards website at: https://www.pcisecuritystandards.org/security_standards/supporting_documents.shtml

For more information on the McAfee PCI Compliance please visit http://www.mcafeesecure.com/us/pci-howitworks.jsp

Capital Confirmation Testing and Monitoring>Daily

Daily tests are run using McAfee SECURE. McAfee SECURE tests Capital Confirmation's web sites daily for vulnerabilities, dangerous content and links that expose consumers' computer and personal information to malicious use. McAfee SECURE helps protect businesses and consumers from hackers, adware, spyware, browser exploits, spammers, phishing attacks and online scams. Here is more information on McAfee SECURE from their website:

> **Automated network security audits combined with an extensive vulnerability management portal.**
> To date McAfee has conducted more than 20 million scans for our customers. Over 80,000 web sites rely on McAfee's daily vulnerability assessments for protection from hackers and third-party certification of their security. Our advanced vulnerability discovery and management technology provides a highly effective security solution with an ROI proven in more than 1,000 published studies.



Vulnerability Knowledge Base

McAfee's up-to-date vulnerability knowledge base powers our comprehensive network security audits and vulnerability management technology. We update the knowledge base every 15 minutes with tests for newly discovered vulnerabilities and validated fixes from hundreds of sources worldwide. These continuous updates, combined with between-scan proactive alerts, ensure McAfee customers are always alerted of the latest vulnerabilities affecting their network.

Vulnerability Management Portal and Alert System

McAfee's vulnerability management portal provides highly secure access to detailed vulnerability audits and remediation information on n-tiered load-balanced application servers. Our web-based vulnerability management portal provides easy access to vulnerability management information from any location. Extensive tools enable you to launch scans, examine vulnerability details, create network device groups, track trends, access patch information, configure alerts, assign user rolls and user device responsibility groups, and generate customized reports.

Scan Appliances

Our network of distributed proprietary scanning servers, located in multiple data centers in North America and Asia, allows us to reliably perform daily security audits for thousands of clients located in more than 40 countries around the world. Each scan appliance is controlled by our central knowledge base and vulnerability management system, allowing the most suitable appliance to be automatically assigned to each device under test.

Data Security

McAfee is the only security scan vendor to be third-party certified to the CISP/AIS Level 1 security standard by Visa International.

Capital Confirmation Testing and Monitoring>Monthly

Monthly testing of the Capital Confirmation service is done using HP's WebInspect. Here is information on HP WebInspect from their website:

> HP WebInspect performs web application security testing and assessment for today's complex web applications, built on emerging Web 2.0 technologies. HP WebInspect delivers fast scanning capabilities, broad security assessment coverage and accurate web application security scanning results.
>
> HP WebInspect identifies security vulnerabilities that are undetectable by traditional scanners. With innovative assessment technology, such as simultaneous crawl and audit (SCA) and concurrent application scanning, you get fast and accurate automated web application security testing and web services security testing."

For more information on HP WebInspect, visit:
https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200%5E9570_4000_100__

Capital Confirmation Testing and Monitoring>Customer / Third-Party Testing

In addition to the testing performed by Capital Confirmation on its own technology security, Capital Confirmation's customers perform initial security and technology due diligence reviews. Included in those tests are security questionnaires, ethical vulnerability and penetration testing, user testing, full code reviews, additional third-party scans, personal background checks, financial reviews, personal credit checks, and multiple site walk-throughs among other tests. Through that battery of tests, every one of Capital Confirmation's Top 15 banks and large accounting firms has moved forward with the Capital Confirmation service. Where there was a recommendation that Capital Confirmation believed strengthened the security of its application, Capital Confirmation implemented the recommendation. In addition to the initial reviews and due diligence, the large banking and accounting firm customers continue to test/scan/monitor the Capital Confirmation security and technology on a scheduled monthly and yearly program with each requiring an annual re-review. Capital Confirmation continues to satisfactorily pass every initial, monthly, and annual re-review for the most demanding of users – the largest banks and accounting firms in the world.