

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > pay.globalline-credit.com

## SSL Report: pay.globalline-credit.com (112.175.106.100)

Assessed on: Tue, 14 May 2019 09:59:05 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

#### Overall Rating

F

#### Certificate

#### Protocol Support

#### Key Exchange

#### Cipher Strength

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server is vulnerable to the [OpenSSL Padding Oracle vulnerability \(CVE-2016-2107\)](#) and insecure. Grade set to F.

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO »](#)

# Certificate #1: RSA 2048 bits (SHA256withRSA)



## Server Key and Certificate #1

Subject	pay.globalline-credit.com Fingerprint SHA256: e569dc82377119d58fe2afb8840721a8bdb90a4456c8df2dc18951d1b578dea8 Pin SHA256: kLvOaaPgUzcr6xJoU30pOvtwF80OsqVhoMGcRk15XE=
Common names	pay.globalline-credit.com
Alternative names	pay.globalline-credit.com www.pay.globalline-credit.com
Serial Number	009e43d14fbc5e6e6543d13ce57bbafc2
Valid from	Thu, 09 May 2019 00:00:00 UTC
Valid until	Thu, 06 Aug 2020 23:59:59 UTC (expires in 1 year and 2 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Domain Validation Secure Server CA AIA: <a href="http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt">http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt</a>
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: <a href="http://ocsp.sectigo.com">http://ocsp.sectigo.com</a>
Revocation status	Good (not revoked)
DNS CAA	No ( <a href="#">more info</a> )
Trusted	Yes Mozilla Apple Android Java Windows



## Additional Certificates (if supplied)

Certificates provided	3 (4751 bytes)
-----------------------	----------------

Additional Certificates (if supplied)

Chain issues

Contains anchor

#2

Subject	Sectigo RSA Domain Validation Secure Server CA Fingerprint SHA256: 7fa4ff68ec04a99d7528d5085f94907f4d1dd1c5381bacdc832ed5c960214676 Pin SHA256: 4a6cPehl7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng=
Valid until	Tue, 31 Dec 2030 23:59:59 UTC (expires in 11 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA

#3

Subject	USERTrust RSA Certification Authority <span>In trust store</span> Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4ITdO/nEW/Td4=
Valid until	Mon, 18 Jan 2038 23:59:59 UTC (expires in 18 years and 8 months)
Key	RSA 4096 bits (e 65537)
Issuer	USERTrust RSA Certification Authority Self-signed
Signature algorithm	SHA384withRSA



Certification Paths



Click here to expand

Configuration



## Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.



## Cipher Suites

### # TLS 1.2 (server has no preference)



TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	<b>WEAK</b>	112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 2048 bits FS <b>WEAK</b>	112
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH sect571r1 (eq. 15360 bits RSA) FS <b>WEAK</b>	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	<b>WEAK</b>	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS <b>WEAK</b>	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	<b>WEAK</b>	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS <b>WEAK</b>	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	<b>WEAK</b>	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH sect571r1 (eq. 15360 bits RSA) FS <b>WEAK</b>	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	<b>WEAK</b>	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS <b>WEAK</b>	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	<b>WEAK</b>	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH sect571r1 (eq. 15360 bits RSA) FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH sect571r1 (eq. 15360 bits RSA) FS	128

## Cipher Suites

TLS_RSA_WITH_RC4_128_SHA (0x5)	<b>INSECURE</b>	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	<b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	ECDH sect571r1 (eq. 15360 bits RSA) FS <b>INSECURE</b>	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	<b>WEAK</b>	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS <b>WEAK</b>	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	<b>WEAK</b>	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS <b>WEAK</b>	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH sect571r1 (eq. 15360 bits RSA) FS <b>WEAK</b>	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	<b>WEAK</b>	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS <b>WEAK</b>	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	<b>WEAK</b>	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH sect571r1 (eq. 15360 bits RSA) FS <b>WEAK</b>	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH sect571r1 (eq. 15360 bits RSA) FS	256
# TLS 1.1 (server has no preference)		<a href="#">+</a>
# TLS 1.0 (server has no preference)		<a href="#">+</a>



## Handshake Simulation

<a href="#">Android 2.3.7</a> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Android 4.0.4</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH sect163k1 <b>FS</b>
<a href="#">Android 4.1.1</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH sect571r1 <b>FS</b>
<a href="#">Android 4.2.2</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH sect571r1 <b>FS</b>
<a href="#">Android 4.3</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH sect571r1 <b>FS</b>
<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 <b>FS</b>
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 <b>FS</b>

## Handshake Simulation

<a href="#">Android 6.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Baidu Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH sect571r1 FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 69 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 70 / Win 10</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 62 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Googlebot Feb 2018</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">IE 7 / Vista</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
<a href="#">IE 8 / XP</a> No FS <sup>1</sup> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA	RC4
<a href="#">IE 8-10 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 11 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">IE 10 / Win Phone 8.0</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
<a href="#">IE 11 / Win Phone 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256	No FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Edge 15 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Java 6u45</a> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA	No FS RC4
<a href="#">Java 7u25</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS

## Handshake Simulation

<a href="#">OpenSSL 0.9.8y</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 2048	FS
<a href="#">OpenSSL 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH sect571r1	FS
<a href="#">OpenSSL 1.0.2e</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 6 / iOS 6.0.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 6.0.4 / OS X 10.8.4</a> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 7 / iOS 7.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 7 / OS X 10.9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / iOS 8.4</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / OS X 10.10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH sect571r1	FS

### # Not simulated clients (Protocol mismatch)

[IE 6 / XP](#) No FS<sup>1</sup> No SNI<sup>2</sup> Protocol mismatch (not simulated)

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

**(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.**



## Protocol Details

### DROWN

No, server keys and hostname not seen elsewhere with SSLv2

(1) For a better understanding of this test, please read [this longer explanation](#)

(2) Key usage data kindly provided by the [Censys](#) network search engine; original DROWN website [here](#)

(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete

### Secure Renegotiation

Supported

#### Secure Client-Initiated Renegotiation

No

#### Insecure Client-Initiated Renegotiation

No

#### BEAST attack

Not mitigated server-side ([more info](#)) TLS 1.0: 0xa

#### POODLE (SSLv3)

No, SSL 3 not supported ([more info](#))

#### POODLE (TLS)

No ([more info](#))

#### Zombie POODLE

No ([more info](#)) TLS 1.2 : 0x000a

#### GOLDENDOODLE

No ([more info](#)) TLS 1.2 : 0x000a

#### OpenSSL 0-Length

No ([more info](#)) TLS 1.2 : 0x000a

#### Sleeping POODLE

No ([more info](#)) TLS 1.2 : 0x000a

### Downgrade attack prevention

Yes, TLS\_FALLBACK\_SCSV supported ([more info](#))

#### SSL/TLS compression

No

### RC4

Yes INSECURE ([more info](#))

#### Heartbeat (extension)

Yes

#### Heartbleed (vulnerability)

No ([more info](#))

#### Ticketbleed (vulnerability)

No ([more info](#))

#### OpenSSL CCS vuln. (CVE-2014-0224)

No ([more info](#))

### OpenSSL Padding Oracle vuln. (CVE-2016-2107)

Yes INSECURE ([more info](#))

#### ROBOT (vulnerability)

No ([more info](#))

### Forward Secrecy

With some browsers ([more info](#))

#### ALPN

No

#### NPN

No

#### Session resumption (caching)

Yes



## Protocol Details

Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1, sect233r1, sect239k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1, secp160k1, secp160r1, secp160r2, secp192k1, secp192r1, secp224k1, secp224r1, secp256k1, secp256r1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 (Server has no preference)
SSL 2 handshake compatibility	Yes



## HTTP Requests



- 1 <https://pay.globalline-credit.com/> (HTTP/1.1 200 OK)



## Miscellaneous

Test date	Tue, 14 May 2019 09:56:20 UTC
Test duration	165.440 seconds

### Miscellaneous

HTTP status code	200
HTTP server signature	Apache
Server hostname	-

SSL Report v1.34.2

Copyright © 2009-2019 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

[Try Qualys for free!](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.