Mortgage servicing excellence

World-class ODC (Offsite Delivery Center) data security for Lending clients

A double security approach to ensuring optimal data privacy

cognizant®

At Cognizant, we take ironclad data security seriously. And it's our top priority in supporting Lending client's servicing and collections operations. To that end, our 360° Security View program ensures ODC (Offsite Delivery Center) data privacy and prevents fraud and threats.
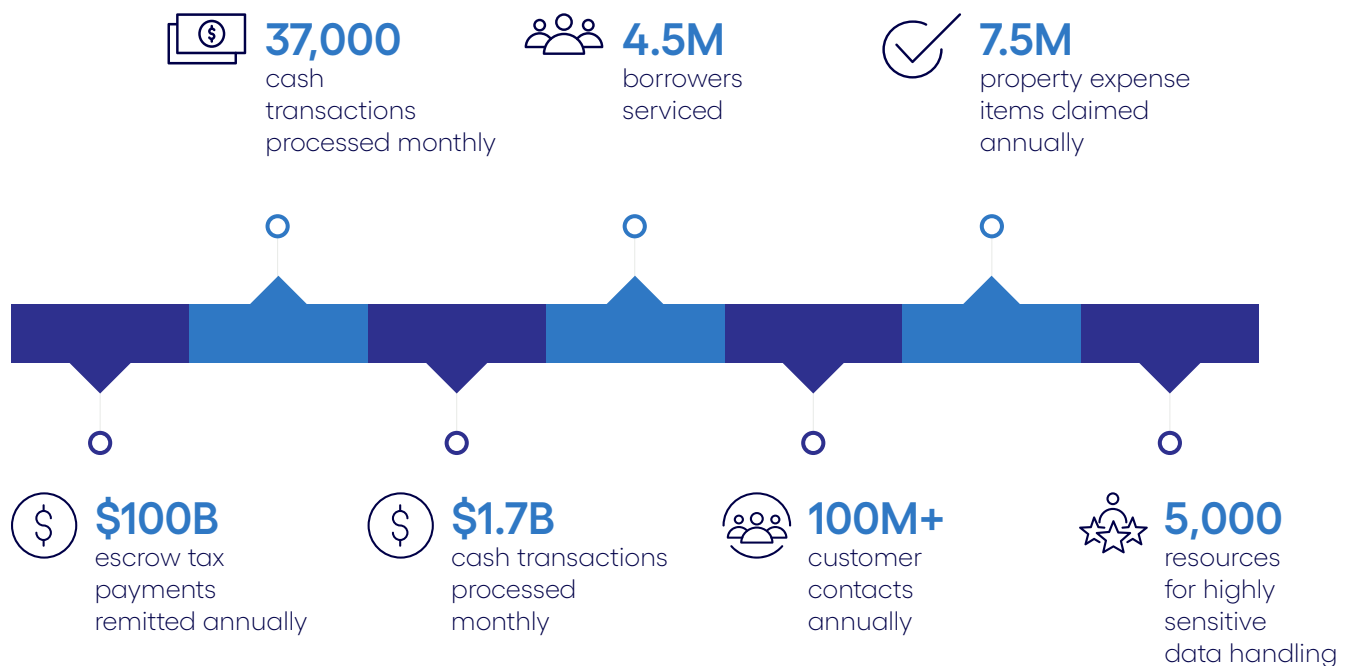
Addressing security requirements for all industry laws, regulations and security mandates, 360° Security View includes all appropriate operational and technological regulations and procedures to safeguard against unauthorized access, loss, destruction, theft, use or disclosure of lending clients's data.

Going well above and beyond industry standards, 360° Security View is proof positive of Cognizant's double security approach to ensuring a reliable and secure information environment for lending clients, its customers, associates and business partners.

Cognizant is an ISO 27001:2013 certified company

Our information security structure is based on the ISMS (Information Security Management System) framework.

Cognizant's ODC prowess by the numbers...

37,000
cash transactions processed monthly

4.5M
borrowers serviced

7.5M
property expense items claimed annually

$100B
escrow tax payments remitted annually

$1.7B
cash transactions processed monthly

100M+
customer contacts annually

5,000
resources for highly sensitive data handling

Our proven resilient, hybrid approach to data security

To protect lending clients and its stakeholders, Cognizant will install our leading proprietary hybrid onsite/remote approach, which has proven successful with multiple lending clients. This flexible solution takes the stringent controls of our 250+ Offsite Development Centers (ODCs) worldwide and duplicates them for remote (i.e., work from home) environments.

This redundancy ensures resiliency and operational continuity in the event of a business disruption—pandemics, outages, natural disasters, etc.—allowing for a smooth, seamless transition from a physical to virtual ODC environment if necessary for uninterrupted service uptime and SLA adherence.

Onsite: Stringent ODC controls and physical oversight

Cognizant's world-class security at our ODCs is unsurpassed in the industry. Customized to our clients' unique needs, KPIs and demands, our facility security protocols range from restricted access to credential/fingerprint/facial recognition…from anti-tailgate controls to intrusion detection…from social media monitoring to travel risk and incident case management. Among our ODC security practices are:

Access control

- **Facility entry and exit points** are staffed by security guards and monitored by CCTV video surveillance, with recordings maintained for at least 30 days
- **Photo ID cards**, issued to all associates, are verified by security guards before allowing access to work areas
- **Biometric and proximity-based access controls** are implemented to restrict access to critical Cognizant data centers.

Equipment security

- **Workstations, cables and network ports** are physically protected from unauthorized access or tampering
- **Unauthorized photography, video recording**, or any other form of image capturing are forbidden in work areas and other critical areas
- **Project-specific printers and cross-cut shredders** are installed at all locations
- **Fire protection systems**—smoke detectors, sprinklers, manual call points, fire evacuation maps, manual fire extinguishers—are installed at all locations.

Visitor access

- **Visitors** are escorted by Cognizant employees or security guards within the facility, then screened as they exit
- **Color-coded lanyards** are issued to contractors, visitors and employees to ease identification.

Remote: Replicating ODCs for work-from-home

To replicate our ODCs' high level of security for Cognizant associates working from home, Cognizant utilizes our "WFH ODC" system. This AI-based tool creates a secure virtual environment that ensures only authorized personnel can access data.

Successfully deployed for multiple key Cognizant clients, WFH ODC safeguards lending clients's data and systems by restricting mobile phone usage, preventing screen captures and increasing vigilance in keeping systems attended. It employs facial authentication, continuously monitoring facial expressions in real time. The system:

- **Captures** only the associate's face in front of their Cognizant-issued laptop; it does not capture or record screen content or background video/audio unless a violation is detected
- **Auto-locks** if unauthorized access to the associate's Cognizant-issued laptop is detected
- **Differentiates** between intentional versus unintentional alerts (e.g., a family member passing by versus someone deliberately looking at the screen).

In addition, detailed incident summary reports monitor for multiple potential security-compromising factors, providing notifications such as:

- Imposter detected
- Associate left session
- Mobile camera detected
- Laptop camera blocked
- Suspicious mobile device activity
- Multiple individuals in front of screen

Additional data security and management measures

In addition to restricting access to ODCs and remote laptops, Cognizant implements multiple security and management protocols to protect lending clients data. No data is stored in the Cognizant network; all work is performed through the lending clients IT network, with robust control measures at logical and user levels. These include:

Logical controls

- **Data transmission** between Cognizant and lending clients is encrypted using technologies such as VPN/Citrix
- **All outgoing emails** are scanned for confidential documents using a data loss prevention (DLP) tool
- **Anti-virus agents**, endpoint compliance and updated patches are installed to ensure the system is safe from virus and malware attacks
- **Network-based IPs** are implemented at all ingress points to monitor network-based attacks
- **External storage devices** (CDs, USB drives, memory card readers) are disabled by default on all systems
- **SIEM technology** facilitates real-time analysis of any security alerts
- **Bit locker encryption**, with industry-standard cryptographic solutions, is enabled on all laptops
- **Security controls**, including password complexity requirements and screen saver idle timeouts, are strictly enforced
- **Firewalls** are configured to deny all non-designated traffic by default
- **Servers and network devices** are hardened based on security best practices
- **Penetration tests** and vulnerability assessments are conducted on a regular basis, and sanitization technology and tools are deployed as needed
- **Anti-spyware** is installed on all ODC desktops and remote Cognizant-issued laptops to protect against malicious mobile codes.

User controls

All Cognizant associates must:

- Submit to a stringent **background check** before joining Cognizant
- Read, understand and sign Cognizant's well-defined **Acceptable Use Policy,** which governs the protection of confidential information
- Sign a **Non-Disclosure Agreement (NDA)** with both Cognizant and lending clients
- Participate in information security awareness **training programs,** with annual refresher courses and lending client-specific briefings.

Cognizant data security controls at a glance

Network and data center/cloud/endpoint security

- ASA/NG FW
- NW reverse proxy
- NW-Anti-DDoS
- Rogue wireless scan
- Cloud security
- AV & anti-spyware
- DLP & EDR
- Email protection
- SWG/web filtering
- SCCM/Mac IOS/MDM

Vulnerability/compliance management

- Vulnerability analysis
- Security compliance
- Website security scanner
- Remote vulnerability scanning
- Penetration testing and security audits
- Source code analysis
- Software vulnerability analysis (automated)
- Security compliance
- Proctoring and live monitoring solution

Data protection/ identity and access management

- Encryption/ data privacy
- MFA, password policy, activity monitoring
- Secure coding SAST/DAST
- Privileged/role-based access management

SOC/analytics/ automation/IR

- Intrusion prevention
- Data leak prevention
- Malware sandboxing
- Endpoint detection and response
- SIEM monitoring
- Threat intelligence
- Automation/ orchestration/ analytics
- Source code analysis
- UFED for PC mobile forensics
- Internet artifact and system forensics
- Forensic investigations

About Cognizant Mortgage Services Corporation

Cognizant's 360° Security View data security program for lending clients is a service of **Cognizant Mortgage Services Corporation (CMSC)**, which provides end-to-end and component-based mortgage solutions to deliver differentiated outcomes to the mortgage industry. A verified financial services provider by Nationwide Mortgage Licensing System and Registry, CMSC complies with the Secure and Fair Enforcement for Mortgage Licensing Act (S.A.F.E. Act) and other federal regulations.

We also invite you to Learn more about our **Mortgage Operations Services** and connect with **Joseph (Joe) Miller, Head of Lending BPS**.

CMSC Offices

Primary Office

8383 Dominion Pkwy
Suite 276W
Plano, TX 75024
Email Address – CMSCinfo@cognizant.com
Contact # 214-459-6929
Toll Free # 888-839-0491

Arizona Branch Office – NMLS # 2109723

1130 North Alma School Road
Suite 200, Room 274
Mesa, Arizona 85201
Email Address –
Michael.Isaacson@cognizant.com
Contact # 214-459-6929
Toll Free # 888-839-0491

Navi Mumbai, Maharastra, India Branch Office – NMLS # 2117558

Mindspace SEZ, Thane-Belapur Road
Building No 9, 5th Floor, Unit 501
Navi Mumbai, Maharastra, India 400708
Email Address – Ritesh.Garg@cognizant.com
Contact # +91 70212 84771
Toll Free # 888-839-0491

Hyderabad, India Branch Office – NMLS # 2173358

Mindspace SEZ, Building No. 12A
Unit No. 901, Madhapur
Hyderabad, Telangana, India 500081
Email Address –
SyedHidayatullah.Aneef@cognizant.com
Contact # +91 97908 79779
Toll Free # 888-839-0491

Chennai, India Branch Office – NMLS # 2250825

SBD 2, 5th Floor, Wing A, B & C
SIPCOT Siruseri IT Park, Padur Post
Siruseri, Tamil Nadu, India 603103
Email Address –
Saravana.KumarK@cognizant.com
Contact # +91 9894402544
Toll Free # 888-839-0491

Honolulu Branch Office – NMLS # 2212428

500 Ala Moana Blvd
Suite 7400 - Office 444
Honolulu, HI 96813
Email Address – Amanda.Farley@cognizant.com
Toll Free # 888-839-0491

Philippines Branch Office - NMLS # 2586636

27th Floor, GIGA Tower,
BridgeTowne IT Park
Ugong Norte, Quezon City, NCR,
Philippines 01110
Email Address: CMSCinfo@cognizant.com
Toll Free # 888-839-0491, Ext 817261/817264

For complaints, please contact us at # 888-839-0491 or Jay.Hinton@cognizant.com.

cognizant®

Cognizant (Nasdaq-100: CTSH) engineers modern businesses. We help our clients modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. Together, we're improving everyday life. See how at **www.cognizant.com** or follow us **@Cognizant.**

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

280 Bishopsgate
London
EC2M 4RB
England
Tel: +44 (01) 020 7297 7600

India Operations Headquarters

5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096 India
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters

1 Fusionopolis Link,
Level 5 NEXUS@One-North,
North Tower Singapore 138542
Phone: + 65 6812 4000

WF 2896150