Overview of Security Practices

Security protects the confidentiality of an account holder's financial information and prevents theft of their assets. It is important to a financial institution and their account holders to know that Digital Banking transactions are private and secure. The sophisticated security architecture of Digital Insight™ Solutions prevents unauthorized users from gaining access to sensitive information.

NCR maintains a security department with a complement of staff members and tools to oversee security functions. Formal policy and procedure are in place to guide activities in this area. Security practices impact all resources owned or operated on behalf of all locations and subsidiaries of NCR as indicated in the following section.

Non-Repudiation

Repudiation in our environment generally refers to an attempt by an end user to refuse payment on the basis that they didn't originate or authorize the payment. NCR protects our clients from such claims by providing a secure environment that authenticates the end user, validates their requests, maintains audit logging, and protects sensitive data from interception/alteration by means of encryption and other security mechanisms. Details regarding the security and integrity of Digital InsightTM Solutions are available in the sections that follow.

Requesting Security-Related Information from NCR

Financial institution clients frequently ask questions to evaluate the state of security of NCR's computing resources and facilities. While this is legitimate and expected, some of the requests that we receive would require us to disclose sensitive information, subjecting NCR and our clients to unacceptable risk. Examples of sensitive information that NCR is not currently at liberty to disseminate includes (but is not limited to):

- Configuration information related to access control mechanisms such as firewalls, intrusion detection systems, and anti-virus systems
- Detailed network diagrams
- Inventories of computing resources and communications equipment
- Information related to operating system configuration, version, or patches installed

- Corporate policy and operating procedure. Summaries of corporate policy and procedure are available on Admin Platform.
- Reports that detail or summarize attempts to breach security, beyond reporting called for by service agreements
- Reports that detail or summarize the performance of access control mechanisms, such as firewalls, intrusion detection systems, and anti-virus systems
- Reports that detail the results of third-party security audits
- Disaster recovery and business resumption procedures. A disaster recovery summary is contained is available on Admin Platform.

Please note that although NCR protects our clients by not disclosing the types of information above to a broad audience, independent oversight is maintained as a result of efforts such as SSAE16 SOC 1 and 2 audits, security testing, and federal examinations. Each of these efforts requires full disclosure of all such information to the reviewing body.

For obvious security reasons, NCR has implemented controls surrounding the disclosure of security-related information. To reduce the risk of disclosing sensitive information, we do not currently support conference calls, open discussion, or other forms of direct communication with security staff. Additionally, management resources responsible for the integrity of NCR's security practices must approve the release of such information.

While NCR has a responsibility to address the risks described above, we also understand the need to provide our clients with the tools they need in support of their vendor management and audit activities.

Financial institution clients can easily get answers to security related questions from the following sources:

Security and Compliance Page in Admin Platform – This page is intended to provide a level of detail that appropriately addresses your vendor management and auditing needs, while protecting the security interests of all NCR clients.

Relationship Manager - If the needed information is not available in Admin Platform please contact your relationship manager. Your relationship manager is committed to ensuring that your needs are properly addressed, and will provide a formal response after reviewing your needs with the appropriate NCR resource(s). If you're not sure how to contact your relationship manager, our Customer Care staff can direct you.

Reporting Incidents to NCR Clients

NCR has documented corporate policies and procedures that provide guidelines for effective incident response, and to ensure that incidents are escalated to the proper levels of authority. The policy includes guidance on the types of intrusions and security breaches that will be escalated to law enforcement and the actions necessary to support the filing of Suspicious Activity Reports (SARs). Customer Care's internal procedures provide additional detail on how an intrusion incident will be communicated to clients.

If an NCR employee becomes aware of a security incident, that employee is responsible for initiating an appropriate escalation procedure per the nature of the incident. The areas within NCR that participate in incident response are required to create and maintain supporting procedures. Procedures describe response activities related to events such as (but not limited to) the following:

- Network-based attacks and intrusion
- Virus and other malicious software
- Theft or destruction of company property
- Abuse or disregard of corporate security policy
- Fraud

The procedures referenced above describe the responsibilities of NCR staff, including (but not limited to) the following:

- Assignment of primary and alternate resources responsible for incident response activities
- Internal status reporting and escalation procedures
- Severity assessment
- Segregation and isolation of threat
- Internal user base communications
- Coordination with law enforcement agencies
- Client communications
- Vendor communications
- Public communications
- Post-event evaluation

NCR Customer Care will provide communications to clients and partners as warranted, including current status, any protective activity required on the part of the client or partner, and final disposition. If notification by email does not pose a security risk, an email will be sent to the financial institution (or to a distribution list, depending on the scope and nature of the incident). If notification by email poses a risk, clients will be contacted by phone. Technical representatives will assist in formulating communications as needed.

Since recovery of NCR computing resources does not involve financial institution participation, activities are generally limited to interaction with end users that may contact the financial institution with questions. The financial institution is encouraged to develop internal procedures that identify internal and external communication responsibilities in support of such events.

NCR does not currently distribute reports detailing attempts to breach the security mechanisms protecting our resources. Given the size of our client base, dissemination of this type of information to such a broad audience exposes us and our clients to unacceptable risk. However, NCR will notify affected clients as required by their service agreements.

Application and Systems Development Practices

A review of NCR systems development and maintenance, and additional information in the area of applications, can be found in the SSAE16 SOC 1 and 2 Reports, which are available in Admin Platform.

We also provide annual summaries of our third-party penetration tests by request. Contact your Relationship Manager to request.