Digital Insight^{TM} Solutions Incident Management

The privacy and security of our customers' data is of the highest importance to us and we consider it key to maintaining customers' trust.

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 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.