BRANCH AUTOMATION SOLUTIONS – ATM AVAILABILITY & SECURITY SERVICE

This exhibit ("Exhibit") describes DN's ATM Availability & Security Service under its Branch Automation Solutions ("BAS") portfolio ("BAS – ATM Availability & Security" or "Service") and is subject to the other terms and conditions that are referenced in the Ordering Document, including other exhibits as applicable. The Parties' Managed Equipment and Services Agreement ("MESA") and its Equipment Schedule incorporate this Exhibit (collectively, the "Agreement"). Capitalized terms used herein and not otherwise defined in the Agreement have the meanings set forth in Section 7 Definitions.

1. SERVICE COMPONENTS

1.1 Overview. BAS – ATM Availability & Security consists of two components: (1) Subscription Software, and (2) Remote Service components. These components work together on Serviced Equipment and the Device Platform, supported by DN's field maintenance services.

Subscription Software. DN will provide, install, and maintain the Subscription Software at each Serviced Equipment during the Subscription Term. The Subscription Software includes the following components:

- Terminal Application Software ("Terminal Software"), such as VCP v7.x ("VCP7"), or Network Solution v7.x ("NS7") or a higher more recent version;
- Managed Security Software; and
- AllConnect Data Engine agent ("ACDE").

Remote Service Components. DN will provide the following remote Service components:

- Monitoring and Event Management;
- Integrated Service Desk;
- Remote Software Deployment/Management; and
- Security Management.

BAS – ATM Availability & Security requires: (a) hardware configuration as follows: DN Series with the EPC_7G Processor and Microsoft Windows 11; DN Series with the EPC_6G Processor and Windows 10 (2021) with Intel extended support drivers; and/or CS Series with the Canyon Processor and Microsoft Windows 10 (2016) (subject to the DCA or other governing master purchase agreement); (b) DN Device Platform (ProBase 1.5.4 or higher); (c) DN's Subscription Software for the Terminal Software (e.g., VCP7.x or NS7.x) and the MS Software (terminal security software) (this Exhibit); (d) DN's connectivity service for all Serviced Equipment, and (e) DN's Second Line Maintenance ("SLM") Service with a Basic Plan or higher, defined at **Service Descriptions**.

1.2 Subscription Software License. The Agreement's Software Terms (MESA, Section 3 and **Online Provisions**) are supplemented as follows:

a. Software Subscription and Scope. The applicable Software Subscription is valid for the duration of the Agreement's Term while Service is active ("Subscription Term") and it includes DN's (i) grant to Client of a subscription license for applicable Subscription Software; and (ii) Software maintenance and standard support of the Subscription Software (collectively, the "Subscription"). The Subscription excludes customizations or any other services out of scope or services extending beyond the Subscription Term. The Subscription Software license set out herein has no impact on Client's Device Platform (perpetual software license) which is governed by the DCA or other master purchase agreement and Ordering Document.

b. License. During the Subscription Term, Client is granted a limited, revocable, non-exclusive, non-assignable, non-transferable, non-sublicensable right and license to use the specified version of the DN Subscription Software on the Serviced Equipment ("License"). DN provides the Subscription Software in object code form only, as licensed software (not sold). The License terms set out in this Exhibit apply to DN's Subscription Software, including any media on which it is received by Client. This Section applies to the Subscription Software's subsequent version(s), any updates,

supplements, and support services. Client will be deemed to have accepted the Subscription Software upon delivery.

c. **License Restrictions.**

(1) **DN Proprietary Information.** Client acknowledges that the Subscription Software and its structure, organization, source code and related documentation constitute valuable trade secret information and proprietary material that is owned by DN or its third party suppliers and that any actual or threatened violation of these terms will cause irreparable damage to DN. Accordingly, except as expressly permitted in this Exhibit, Client will not:

- Make unauthorized copies of the Subscription Software;
- Allow use of the Subscription Software other than for the permitted use specified in this Exhibit;
- Distribute, sell, rent, transfer, lease, lend, sublicense, loan, assign, pledge, grant a security interest in, or otherwise make available the Subscription Software or any part or copies thereof to any third party, unless otherwise permitted by DN in writing;
- Use the Subscription Software in any service-bureau, timesharing, outsourcing, fee-for-service arrangement or other unauthorized manner;
- Combine or merge the Subscription Software with or into another software or incorporate any Subscription Software or portion thereof into any compilation;
- Disassemble, decompile, reverse engineer or otherwise attempt to derive the structure, sequence or organization of source code, except as permitted by applicable law to achieve interoperability with other software if DN does not offer the means to do so;
- Disable any Subscription Software feature that enables DN to monitor usage levels;
- Remove or alter product identification, copyright, trademark or other proprietary markings contained in or on the Subscription Software or documentation;
- Modify, adapt, recast, transform or otherwise prepare a derivative work of a Subscription Software or portion thereof; or
- Otherwise use the Subscription Software or permit any third party to do any of the foregoing.

(2) **Subscription Expiry or Early Termination.** Prior to any termination of the Subscription Term, and subject to the Parties' mutual agreement, Client, at its expense, may engage DN to remove or disable the Subscription Software from the Serviced Equipment; or certify in writing that Client or its DN-approved agent has removed the Subscription Software from the Serviced Equipment. If Client intends to continue operating the Terminal Software, Client must procure an alternative software license along with or inclusive of the software maintenance and standard support services, pursuant to the DCA or other master agreement and Ordering Document.

2. SERVICE SCOPE

2.1 Service Scope. BAS – ATM Availability & Security encompasses Remote Services, specified as:

a. **Monitoring and Event Management.** DN will provide remote, 24/7 monitoring of Serviced Equipment to identify, classify, and address ATM status data and Error events. Depending on the event classification (critical or non-critical) and potential Error type, DN, through its monitoring tool(s) (MS Software), may act remotely (e.g., attempt an automated self-healing action or a generate ticket for a service call) or create a Ticket for an Incident that flows to DN's Integrated Service Desk or the Field Service Team.

- DN will ensure its monitoring tool(s) transmit the applicable information in near real time from the Serviced Equipment to DN's data center. Client may access the information at Client's account in DN's Managed Service Customer Portal.

b. **Integrated Service Desk.** DN will provide a single, centralized source to manage the logging, tracking, and dispatching of Incidents or events received verbally from a Client representative (e.g., branch employee or Client-owned helpdesk) or remotely from an approved channel ("Support Channel"), such as phone, e-mail, ACDE, other client interface, or from DN's monitoring tool(s).

- DN will perform remote diagnostic operations, including basic call logging, routing, and dispatch to in-depth second line remote support and remote Resolution.

c. **Remote Resolution Service.** DN will attempt a remote Resolution to an Error or event by way of the remote command execution ("Remote Command Execution"). Upon a qualifying Error or event, the Remote Command Execution will run predefined tasks on the Serviced Equipment or for the Software distribution.

d. **Remote Software Deployment / Management.** DN will provide the remote deployment of software updates or patches to the Subscription Software specified on the Equipment Schedule and Client's Device Platform Software and respective operations system provided by DN under the Parties' DCA. Through its Software Deployment Service, DN will create a deployment plan for the critical or high software updates or patches through to the plan's execution. The remote deployment service excludes Client's non-DN provided software that Client maintains, unless otherwise agreed to in writing and specified on the Equipment Schedule.

e. **Customer Portal.** DN will provision and provide access to the Customer Portal. Information stored within the Customer Portal is segregated by Client account and accessible by a secured log in and password. DN will direct to the Customer Portal certain available information for Inventory Management and Electronic Journal ("EJ").

(1) **Inventory Management.** DN will ensure that relevant fleet-wide data or information, such as hardware configuration or software component data, is directed, stored, and available to Client in the Customer Portal, subject to Client's access rights and the Subscription Software. Inventory Management's relevant data will include Payment Card Industry, EMVCo, Microsoft Patch Level and other inventory or relevant data required for legal or compliance assessment.

(2) **Electronic Journal.** DN will ensure the individual Serviced Equipment's financial data or information for each transaction is uploaded on a daily basis and stored as an EJ within the Customer Portal for a minimum 120 day period. Any Client-requested alternative or extended retention period beyond 120 days, unless required by law, will be considered subject to a Change Request Order. Client may access and use the information within the EJ, provided Client will independently cause and instruct its applicable transaction processor to mask the consumer primary account numbers ("PANS") subject to PCI standards. Within the confines of PCI compliance, DN will provide reasonable support for Client's ad hoc requests to assist with the EJ data or information.

f. **Security Management.** DN's Security Management components include: (i) Core Security; (ii) Hard Drive Encryption; (iii) Windows Password Management; and (iv) BIOS Password Management, specified in this Section. DN will manage and update, as needed, the MS Software used for Security Management, which will meet the industry standard for security-related services at the Serviced Equipment. Through its Security Management and MS Software, DN provides a defense against certain known logical or physical vulnerabilities or attacks to the Serviced Equipment. However, DN is not responsible for matters or actors beyond DN's control or knowledge, including physical attacks, environmental, or Location matters or unknown logical attacks.

(1) **Core Security.** DN will provide security management to protect Serviced Equipment from known malware and network-based threats to the Serviced Equipment as well as to comply with applicable ATM requirements of the PCI-DSS. The collective Core Security components include as follows:

- **Anti-Malware.** DN protects the Serviced Equipment's Software against known forms of logical exploits, vulnerabilities, abuse, and malicious software.
- **USB and External Device Control.** Excluding DN-authorized devices at the Serviced Equipment, DN blocks known unauthorized usage of USB ports or external storage mediums, or devices at the Serviced Equipment and logs the respective events.
- **Managed Firewall.** Excluding the authorized network traffic (bidirectional access or usage) to the Serviced Equipment, DN blocks known unauthorized network access or usage and logs the respective attempted access or usage events.
- **24 x 7 Security Alerting.** DN collects and aggregates log data generated across the Serviced Equipment components such as firewalls, anti-malware, and USB controls using predefined monitoring and event management rules to generate alerts, some of which DN sends (e.g., email) to Client subject to the terms in Section 5.
- **Audit Logging and Retention.** DN records and retains all logged information in accordance with the PCI-DSS requirements.

(2) **Hard Drive Encryption.** DN provides a secure boot process and (de)encryption of the internal hard drive of the Serviced Equipment. DN will remotely manage and monitor the encryption status, prevent known attempts for unauthorized access to all (including legally protected) data stored on the Serviced Equipment hard drive while the Serviced Equipment has been Powered-Off.

(3) **Windows Password Management.** DN manages the local Microsoft Windows administrator passwords and password security at the Serviced Equipment. Access to the self-service terminals

Windows administrator password is granted to authorized DN Services personal based on the principle “Need to Know” – “Need to Have” via the respective DN console.

(4) **BIOS Password Management.** DN manages the BIOS password on DN Series type Serviced Equipment and provides BIOS Password Lifecycle Management. Restrictions may apply based on the compatibility of Serviced Equipment’s PC-Core chipset with PCI DSS. The BIOS Password Management Service component is not available on CS Series with Canyon Processors.

g. Entry Level Marketing. DN will provide an attract loop, a static set of imagery and receipt content to be delivered to the Serviced Equipment. The content includes attract loop, please wait, and thank you screens, receipt header and receipt coupon. DN will deliver up to one (1) update per calendar monthly period to the Serviced Equipment.

2.2 Software Agent Install. During the implementation phase, DN will install the necessary Subscription Software (e.g., VCP 7 or NS7, and/or monitoring tools) at the Serviced Equipment. The Subscription Software (the applicable Terminal Software, MS Software, or ACDE) is provided on a subscription basis for the applicable Subscription Term.

2.3 Compliance. DN will ensure that the DN environment, including DN’s system, tools, and services comply with applicable legal or industry standards (for example, PCI-DSS; SOX; and ISO 20001) as applicable to the Serviced Equipment. Subject to the General Conditions Exhibit, Client will ensure that its environment, systems, and operations comply with the applicable legal or industry standards, including PCI governance.

2.4 Hours of Coverage. DN will operate BAS – ATM Availability & Security on a twenty-four (24) hours, seven (7) days a week basis, excluding scheduled downtime, which may differ from the SLM Service or other services specified on the Equipment Schedule or Ordering Document.

3. ADDITIONAL SERVICES, OUT OF SCOPE SERVICES, AND EXCEPTIONS

3.1 Additional Service Options. The additional services, set forth below, are supplemental and subject to a separate Ordering Document or amended Equipment Schedule.

a. Companion BAS offerings, subject to an independent service description, include:
- BAS – Transaction Automation
- BAS – Transaction Assist
- BAS – ATM Cash Optimization
- Any BAS offering for Teller Cash Recycler Services

b. Hardware-related service, e.g., hardware maintenance services.

c. Cash-related services, e.g., provisioning, forecasting, replenishment of cash.

d. Transaction authorization and processing.

e. All software-related services outside the scope of BAS – ATM Availability & Security (Section 1).

3.2 Out of Scope Services. Excluded from the Service are any request for (i) Additional Services; (ii) tasks not specified in this Exhibit’s Section 1; or (iii) deviations from DN’s standard Service offering for BAS – ATM Availability & Security. To the extent permissible or acceptable, DN will respond to approved requests on an ad hoc basis and invoice in arrears the Service at DN’s then-current time and materials rates, unless otherwise agreed to in a proposal or Ordering Document. The Parties may use a Change Request Order to adjust the scope. Examples of out of scope requests includes:

a. Services for management, distribution or installation or deployment of software or software agents or services outside the defined scope of BAS – ATM Availability & Security;

b. Services on legacy or incorrect hardware, e.g., non-DN units or legacy units that are incapable of supporting the standard Service;

c. Any Service request that materially impacts a security standard within DN’s system is prohibited;

d. Any Service request that materially impacts a security standard within Client’s system or the Serviced Equipment will require a Change Request Order with a waiver and hold harmless terms.

3.3 Exclusions to the Service Scope. DN’s Services and performance metrics will exclude:

a. Service required because of events beyond DN’s control or caused by a person or entity other than DN, such as service requests for errors caused by Client’s patrons, staff, or other (non-DN) vendor errors; abuse or misuse of the Serviced Equipment; electrical storms; power failures or fluctuations; failure to follow user maintenance and operating instructions; or the failure of Client’s interconnected

equipment, software, or data outside of DN's management and control (e.g., Client's wiring, conduit, or voice or data transmission equipment or facilities);

b. Services required or impacted by lockouts or damages caused by war, public disorder, vandalism, illegal activity, fire, water or other liquids, burglary, blasting, mining, settling of foundations, expansion of doors or walls, loss of combinations or by imperfect changing of combinations or time locks;

c. Services required because of contact, modification, service, inspection, or tampering with the Serviced Equipment by non-DN designated personnel, relocation of the Serviced Equipment, changes to configuration, software or data, installation of additional features, options or functions; major overhauls, or refurbishing the Serviced Equipment;

d. Malfunctions resulting from the use of software, media, supplies, and/or consumables that DN does not furnish or approve;

e. Service on Serviced Equipment, components or other items that are no longer supported by DN or the manufacturer;

f. Client's failure to perform obligations as set forth in the Agreement (including this Exhibit) to the extent such failure affects DN's ability to perform the Services;

g. Time scheduled for maintenance in accordance with the Agreement, or as part of an approved change where the Parties agreed to a downtime schedule;

h. DN not having direct access to the Serviced Equipment or an adequate process to access the Serviced Equipment upon DN's request;

i. Service requested for no apparent problem, malfunction, or issue with the Serviced Equipment.

4. TRANSITION AND ONBOARDING

4.1 Order to Implementation. In addition to the General Requirements exhibit, BAS – ATM Availability & Security onboard transition will depend on the Client's status with DN's Services.

a. Transition Plan (Legacy Service to BAS – ATM Availability & Security). Prior to transitioning from legacy Services to BAS – ATM Availability & Security, DN and Client will agree in a written transition plan ("Transition Plan") on the necessary steps, responsibilities to transition any Location and Service Equipment to BAS – ATM Availability & Security. The Parties will prepare a complete hardware, software, network and service inventory with an objective to identify and resolve any incompatibility between the legacy Services and BAS – ATM Availability & Security.

b. Onboarding Plan (New Client). Prior to any Remote Services, DN and Client will agree in a written onboarding plan ("Onboarding Plan") on the necessary steps in order to bring BAS – ATM Availability & Security into operations within Client's environment, including DN's telecommunications requirements. An Onboarding Plan will encompass key activities such as:

- DN's review of sales order and associated documentation.
- Kick-off call(s) with Client's assigned contacts and DN's transition team.
- Technical call(s) for Client's to review network, hardware specifications and configurations.
- Agreement on escalation thresholds and contact protocols.
- Agreement on supported DN Series models and configurations in scope for the Service
- Agreement on minimum required hardware and network bandwidth for connectivity.
- Agreement regarding branding and user experience (user interface).
- If applicable, Client provisioning of infrastructure documentation and network topology.
- Scheduling and execution of software agent installations and field team readiness.
- Verification of installation and confirmation of deliverables.
- Issuance of completion form (CFIN) to finalize service activation.

4.2 Master Data. The Parties will compile the requisite Master Data during the onboarding process. Examples of the Master Data include:

- Hardware model
- Hostname
- IP Address
- Terminal ID
- Contact name, phone, email
- Site ID
- Site Name and Street Address
- Serial number
- Escalation Levels
- Notification Hours
- Hours of Coverage
- Contact name, phone, email

5. SERVICE PREREQUISITES

The prerequisites set forth below must be implemented prior to engaging BAS – ATM Availability & Security.

5.1 **Technical Requirements**. BAS – ATM Availability & Security requires prerequisites as follows:

a. DN Series Equipment with corresponding hardware specifications as approved and detailed in the respective Transition Plan or Onboarding Plan.

b. Device Platform (perpetual software licenses) obtained under the DCA or other master agreement:
- Microsoft Windows Operating System.
- Latest and applicable version of Device Platform, e.g., ProBase.

c. Minimum required network bandwidth per link (not aggregated) of 10Mbps for all Serviced Equipment and DN connectivity service as defined or specified during the transition and onboarding process that supports the following minimum network performance standards:
- Throughput = 10Mbps down, 5Mbps up
- RTT Latency = 150 milliseconds maximum
- Jitter = 40 milliseconds maximum
- Packet loss = 0.5%
- Bandwidth usage = 3.5GB

d. Subscription Software:
- Terminal Software: Vynamic Connections Points Client Software Application (VCP-Pro 7.x or Network Solutions 7.x – subscription software license).
- MS Software: Software required for the Remote Services and Client use of the Customer Portal (subscription software license).
- ACDE agent enabled at Serviced Equipment (subscription software license).

5.2 **Service Requirements.** BAS – ATM Availability & Security requires the related exhibits listed below:

a. General Conditions Exhibit

b. SLM Service Description Exhibit, along with the applicable Cash Claims and Liability Exhibit

5.3 **Client Obligations.** In addition to the other Service requirements, Client shall:

a. For VCP 7.x implementations, Client is responsible for host/switch integration and certification of the VCP 7.x terminal software prior to subscribing to the Service.

b. Engage DN's SLM and related hardware services subject to the applicable Service Descriptions as indicated on the Equipment Schedule.

c. Prohibit any unauthorized access to the Serviced Equipment (e.g. remote access, third party file or content distribution, or changing of any software or software configuration on the Serviced Equipment).

d. Permit free and clear access to the Serviced Equipment either for DN's field technicians (onsite access) or DN's Service Delivery personnel (remote access) via the Customer Portal.

e. Ensure the minimum hardware and bandwidth requirements defined during transition planning/onboarding are met (which may vary based on fleet size).

f. Maintain the appropriate processes and systems (as DN advises) to enable the BAS – ATM Availability & Security, which processes and system may require facilitating periodic decisions regarding the appropriate infrastructure and service or software updates or changes.

g. Upon request, certify its adherence to connectivity requirements defined in this Exhibit.

h. Accept and implement pre-defined firewall rules between the Serviced Equipment and DN to allow for monitoring and management.

i. Provide Remote Connection between DN managed services system and Client's network specific to the Serviced Equipment.

j. Perform full system back-ups prior to the commencement of the Services.

k. Permit DN's install or removal of the Subscription Software at the Serviced Equipment, as needed, for the Services throughout the Agreement Term. Prior to the Agreement's expiry or termination, Client will be responsible for removal of the Subscription Software or, for the Terminal Software, a separate agreement for a revised license and software maintenance and standard support subject to the License terms at Section 1.2.

l. Maintain login protocol for the Customer Portal.

m. Ensure that the BIOS password (existing pre-engagement) for the Serviced Equipment is available to DN in order for DN to commence Services.

5.4 If Client does not engage and maintain the service prerequisites, DN will be relieved from any performance metric evaluation, KPI targets, or any other obligation under this Exhibit.

6. SERVICE REPORTING AND KEY PERFORMANCE INDICATORS

Any applicable Service Levels or Key Performance Indicators are specified in the Ordering Document.

7. DEFINITIONS

"**AllConnect Data Engine**" or "**ACDE**" means the DN-deployed software agent, included in DN's Subscription Software, used for diagnostic data comprising low-level, non-PCI machine technical information (e.g., consumption of energy of certain hardware components) that DN uses for maintenance or services and requires for BAS – ATM Availability & Security. ACDE is subject to a subscription software license.

"**BAS – ATM Availability & Security**" means the specific BAS offering described in this Exhibit.

"**BIOS Password Lifecycle Management**" means the management of the BIOS password according to industry standards, e.g., PCI, ISO, etc.

"**Change Request**" means a change requested by either party to an Ordering Document or this Exhibit that is in effect, for products, software or services not otherwise covered in such agreement, the documentation and negotiation of which is accomplished through DN standard change control process. A Change Request may be required for unforeseen circumstances or Client requests.

"**Change Request Order**" means a mutually signed Ordering Document that results from a Change Request where the Parties agree to modify or supplement the service scope, service conditions, service-related fees, Term, or any other terms having a direct impact on the Services.

"**CS Series**" means a specific DN model family of the DN manufactured Serviced Equipment (ATM) required for BAS – ATM Availability & Security.

"**Customer Portal**" means DN's secure web-based centralized hub that permits or collects data or information flowing from Client's Serviced Equipment and DN's monitoring tool(s) regarding Client's Serviced Equipment.

"**Device Platform**" means DN's base or XFS Software loaded on the Equipment. The Device Platform Software is subject to a perpetual software license as governed by the Parties' DCA (or other master purchase agreement) and Ordering Document. The Device Platform is excluded from DN's Subscription Software.

"**DN Series**" means a specific DN model family of the DN manufactured Serviced Equipment (ATM) required for BAS – ATM Availability & Security.

"**Error**" means the Serviced Equipment becomes inoperative or shows abnormal conditions to materially conform to the applicable specifications.

"**Field Service Team**" means DN's field technician team that responds on site to resolve Tickets or Errors subject to the requisite, applicable Services, e.g., SLM, specified on the Equipment Schedule or pursuant to an Ordering Document.

"**Hours of Coverage**" means, unless otherwise agreed upon in an Ordering Document, the days and times that DN is required to provide BAS – ATM Availability & Security, which under this Exhibit is DN will operate BAS – ATM Availability & Security on a twenty-four (24) hours, seven (7) days a week basis, excluding scheduled downtime. The applicable Hours of Coverage may differ from the coverage requirements for Client's SLM Service or other services specified on the Equipment Schedule or Ordering Document.

"**Incident**" means an unplanned interruption to the Serviced Equipment or reduction in the quality of the performance or operability of the Serviced Equipment communicated to DN through the Support Channel.

"**ISO**" means the International Organization for Standardization.

"**License**" has the meaning set forth in Section 1.2(b).

"**Managed Security Software**" or "**MS Software**" means the DN-deployed remote managed security-related Software, included in DN's Subscription Software that is required for the remote Service components for BAS – ATM Availability & Security.

"**Microsoft Windows**" means a particular or given variants of the Microsoft Windows Operating System.

"**Ordering Document**" means the document executed by Client that identifies the specific quantities, charges, and other applicable terms and conditions (including other exhibits) of Client's order of DN products, software and/or services, as they relate to this Exhibit. An Ordering Document may include a Change Request Order.

"**PCI**" and "**PCI DSS**" means the Payment Card Industry and the Payment Card Industry Data Security Standards.

"**Powered-off**" means when the Serviced Equipment has had its power supply manually switched off or remotely shutdown.

"**Remote Connection**" means the bidirectional (two-way) transmission of data between the Serviced Equipment and DN services platform used to remotely identify Error source, resolve Incidents, and monitor the health of the Serviced Equipment.

"**Remote Services**" means DN's distant activities conducted via an electronic connection between DN and Client to analyze the cause of an Error or Ticket and return Serviced Equipment to a normal state of operation without an on-site service call.

"**Resolution**" means a conclusion to an Error or Ticket, either remotely or on-site, or a final DN determination that otherwise closes the Ticket.

"**Security Best Practice**" means industry (self-service industry) or security best practice such as Microsoft, National Institute of Standard and Technology (NIST), European Association for Secure Transactions (EAST), and EUROPOL.

"**Serviced Equipment**" means the connected hardware, e.g., ATM, that is specified on the Equipment Schedule for the applicable DN's Services hardware required for BAS – ATM Availability & Security.

"**SOX**" means Sarbanes-Oxley Act.

"**Subscription Software**" means the components of DN-deployed Software specified in this Exhibit, at Section 1, including the Terminal Software, MS Software, and ACDE as required for BAS – ATM Availability & Security. Subscription Software excludes the Device Platform Software (perpetual license) or any other software not specified in this Exhibit and on the Equipment Schedule.

"**Support Channel**" means the channel that a client uses to log Tickets and track Tickets to Resolution. DN offers dedicated managed service specific e-mail, phone, and web-service (Diebold Nixdorf Portal) options for the authorized Support Channel, to be determined in the applicable Onboard Plan or Transition Plan. Upon request, DN may offer the option to interface with DN's incident management system.

"**Terminal Application Software**" or "**Terminal Software**" means a DN-deployed layer of terminal application Software, e.g. VCP7 or NS7, included in DN's Subscription Software that is required for BAS – ATM Availability & Security.

"**Ticket**" means a distinct record for an Incident in DN's incident management system.

"**VCP**" means Vynamic Connection Points.