Schedule 14
Fraud Detect Schedule

This Fraud Detect Schedule (**Schedule**) effective _____ (**Effective Date**) supplements the Payment Solutions Agreement (the **Agreement**) among State of North Carolina (**Company**) and First Data Merchant Services LLC (**First Data**). Capitalized or other defined terms used, but not defined in this Schedule, have the meanings given to them in the Agreement.

1. Fraud Detect Services

1.1 First Data will provide Company with services to help identify Fraud Detect Transaction Events that are likely to be fraudulent (**Fraud Detect Services**). First Data will provide the Fraud Detect Services using (1) supervised machine learning capabilities that use and analyze Company's Fraud Detect Data (defined in Section 1.6), including information from or about and across consumers' computers or mobile devices, and may also use similar data from other Fraud Detect Services customers in the analysis, and (2) a real-time fraud rules engine, which uses fraud rules determined in consultation with Company. **Fraud Detect Transaction Events** means the digital payment transactions or card or user registrations within the United States to which the Fraud Detect Services will be applied (as indicated in the Implementation Form).

1.2 The Fraud Detect Services will provide Company with: (1) Fraud Detect Responses, and (2) access to a **User Interface** to: (a) review each Fraud Detect Response and resolve a Fraud Detect Response, if desired, (b) obtain fraud analytics, and (c) create and obtain reporting about Fraud Detect Responses and Fraud Detect Transaction Events (report contents will vary depending on the data elements that Company provides or makes available to First Data in connection with the Fraud Detect Services). **Fraud Detect Response** means a real-time automated score that consists of an "allow" or "prevent" recommendation response OR an "allow", "prevent" or "review" recommendation response, as selected by Company, for each Fraud Detect Transaction Event.

1.3 The Fraud Detect Services are a fraud detection tool. The data provided to Company by the Fraud Detect Services do not constitute 'consumer reports' under the Fair Credit Reporting Act (**FCRA**) (15 U.S.C. sec 1681), as amended. Company may use the data provided by the Fraud Detect Services solely for purposes of detecting and preventing fraud. Company certifies and agrees that it will not use the data provided by the Fraud Detect Services as a factor in establishing a consumer's eligibility for credit, insurance, employment or other FCRA purposes.

1.4 *Reserved*.

1.5 First Data will implement the Fraud Detect Services according to the terms and selections identified in the Implementation Form substantially in the form of Exhibit A (**Implementation Form**), which the parties will use commercially reasonable efforts to complete and sign within 30 days of the Effective Date. The Implementation Form defines the scope of the Fraud Detect Services, each party's respective implementation responsibilities, and acceptance criteria and testing timeframe for the Fraud Detect Services.

1.6 In order for First Data to implement and provide the Fraud Detect Services, Company must provide or make available to First Data the card registration, payment transaction and related ancillary data described below for each attempted Fraud Detect Transaction Event (collectively, **Fraud Detect Data**). Company is solely responsible for securely transmitting Fraud Detect Data to First Data using the format and specifications First Data provides. First Data will notify Company of any changes to its data transmission format or specification requirements, which will become effective after receipt from First Data.

Fraud Detect Data:

Merchant Data		
Merchant ID (MID)	Merchant Category Code (MCC)	
Consumer Data		
Customer ID (unique number generated by Company)	Registration time	Telephone Number
Email Address	Name	
Payment Method Data		
Card last four digits	Cardholder billing address*	Registration time
Method Type (card brand or wallet type)	Cardholder name	Instrument ID (PAN first 6 and last 4, token number or Paypal payor ID

		number)
Successful registration (Y/N)	Card BIN	
Order Data		
Order ID	From (location) (store fulfilling the order)*	Creation time
App platform	To (location) (ship to address)*	Price
Currency	Market (territory or brand)	Company's App name
Items	Seller ID (specific Company store number)	Company's App domain
Item Data		
SKU	Quantity	Price
Name	Category	Currency
Transaction Data		
Transaction ID	Time	Gateway reference or ID number (generated by the gateway)
Amount	Type	
Success (Issuer approval or decline)	Gateway Name	
Location Data*		
Latitude + longitude (may be derived from street addresses and postal codes provided by Company)	Postal code	Street 1+Street 2 + City +Locality+ Region + Country
Chargeback Data (First Data to provide if First Data provides acquiring services for Company)		
Transaction ID (or Gateway reference)	Dispute time	Currency
Gateway	Status	
Non Fraud	Amount	
Device Data Elements Generally		
Device ID (for device used to initiate a Fraud Detect Transaction Event)	Device type (phone (Android/ios, desktop, ipad)	IP address (of device at time of Fraud Detect Transaction Event)
Session ID	Geo Location (latitude + longitude + altitude of device at time of Fraud Detect Transaction Event)	Operating System and Version
Fingerprint Source (identifier for platform submitting device data)	Time zone information (offset to UTC in hours and time zone string)	
ios/Android Device Data Elements		
Device properties (Emulator or jailbreak status (Y/N))	Device info (manufacturer, model)	Fonts installed on device
Timestamp	Android or ios ID	Customer ID
System language	Carrier information	Screen information (resolution, scale, height and width)
Carrier information (country, type, operator ID and name)	Country/Operator of SIM card	Mobile Country Code of operator
Mobile Network Code of operator	Location access status (permission granted to app)	
Browser Data Elements		
URL	Language	Color Depth
Display (pixel, resolution, available resolutions)	Does session or local storage occur (Y/N)	Browser platform
User agent	Language set by browser	Does browser support Indexed Database or Open Database (Y/N)
Do not track enabled (Y/N)	Plug Ins (name, description)	MIME types
Ad blocker software enabled (Y/N)	Spoofing (browser language, screen resolution, OS, browser)(Y/N)	Max # of touchpoints if mobile device
CPU information (class of CPU and # of cores)	Browser name	Fonts available

Does browser support Canvas or webGL APIs (Y/N)	Could a touchpoint be created (Y/N)	Is Touch start available (Y/N)

1.7 To enable Company to provide the device data elements listed in Section 1.6 to First Data, (1) First Data will provide Company with Software for Company's use subject to the terms of this Section 1.7, or (2) Company may obtain and use device intelligence software from its own third party service providers. **Software** means the software application, including any APIs or SDKs, which collects information from or about Company's mobile apps and/or websites end-users' computers or mobile devices.

1.7.1 If Company desires to use the Software, First Data grants Company a nontransferable, nonexclusive, limited license only during the time period in which First Data provides Fraud Detect Services to Company to: (1) permit Authorized Users to install or integrate the Software into Company's mobile apps and/or websites (and use the SDKs to assist in such integration) solely to facilitate Company's use of the Fraud Detect Services; (2) use the Software solely as integrated into Company's mobile apps and/or websites to use the Fraud Detect Services; (3) permit Authorized Users to make a limited number of copies of the Software user documentation for Authorized Users' internal use as needed to install or integrate the Software into Company's mobile apps and/or websites, and/or operate the Software as part of Company's mobile apps and/or websites; and (4) permit Company's mobile apps and/or websites end-users to use the Software solely as an integrated part of Company's mobile apps and/or websites and not on a stand-alone basis. **Authorized Users** means those individuals who are specifically designated (by password or other use identification) to use the Software, and may be Company's employees or its contractors under disclosure obligations to Company substantially similar to those in the Agreement. Company is responsible for ensuring any use of Software Materials by Authorized Users is in accordance with this Section 1.7.

1.7.2 Except as explicitly provided in this Section 1.7 or as expressly permitted by applicable law, Company shall not, and shall not permit or authorize third parties to: (1) copy, modify, translate, enhance, decompile, disassemble, reverse engineer, or create derivative works of the Software Materials; (2) rent, lease, or sublicense the Software Materials; (3) use the Software Materials on a service bureau or application service provider basis; (4) provide, divulge, disclose, make available to, or permit any third party's use of the Software Materials; or (5) circumvent or disable any technological or security features or measures in Software Materials, including to attempt to discern the source code for Software. **Software Materials** means, collectively, the Software and Software user documentation.

1.7.3 Upon termination of the Fraud Detect Services for any reason, unless otherwise instructed, Company must immediately cease all use of the Software Materials and return them to First Data.

1.8 Company is solely responsible for determining if the Fraud Detect Services and Company's Settings satisfy its business, legal, or network scheme requirements. **Company's Settings** means the instructions, settings, options, rules, requirements, strategies, or other instructions related to the Fraud Detect Services that Company provides, selects, or acts upon (or that are provided, selected, or acted upon at Company's direction).

1.9 First Data may terminate the Fraud Detect Services if its rights or access to third party technology or software used to provide the Fraud Detect Services is terminated or ends.

1.10 ***First Data disclaims all warranties (express or implied) that the Fraud Detect Services will accurately identify every instance of fraud or that every transaction identified as fraudulent is, in fact, fraudulent. Company is solely responsible for Company's Settings and all decisions it makes or actions it takes or does not take (or are made or taken or not taken at Company's direction) on Fraud Detect Transaction Events.***

1.11 ***The Fraud Detect Services described in this Schedule are provided by First Data and not the Bank. The Bank has no performance obligations or liabilities to Company in connection with the Fraud Detect Services***.

1.12 Company agrees to take all preparatory steps to start its implementation of the Fraud Detect Services no later than _____.

2. Support. First Data will provide Company with the following support for the Fraud Detect Services:

(1) Severe Issue Support. For severe technical issues, Company may contact the First Data Global Command Center at +1 800-555-9966 on a 24/7/365 basis.

(2) Production Support. Production support for frequently asked questions (**FAQ Support**), issue triage, and escalations to application support and unblocking is available by contacting First Data's relationship team. Production support is also available by email to FraudDetectSupport@firstdata.com. Production support may be provided at varying hours of operation depending on the access point's standard operating business hours.

(3) Implementation Manager. An implementation manager will assist with implementation, integration, and production readiness for the Fraud Detect Services (**Implementation Manager**). During the implementation process, Fraud Detect Services support will be provided by the Implementation Manager.

(4) Portfolio Manager. During implementation and continuing post-implementation, a non-dedicated portfolio manager will periodically provide macro-level fraud trend analysis and suggestions designed to enhance Company's overall fraud prevention and risk strategy.

3. Data Usage

3.1. First Data may retain, use, and share the Fraud Detect Data that Company provides or makes available to First Data in connection with the Fraud Detect Services, including personally identifiable information, to provide the Fraud Detect Services; for product development, analytics, and reporting; and as described in the Fraud Detect Privacy Statement. First Data's Fraud Detect Privacy Statement is available at https://www.firstdata.com/en_us/products/merchants/security-and-fraud-solutions/fraud-detect-solutions.html.

3.2. Except for the limited license granted in Section 1.7, Company obtains no rights or license to First Data's models, products, services, or data generated by them, and Company reserves all rights to the foregoing not expressly granted to Company.

4. Data Privacy

4.1 When First Data uses Company's Fraud Detect Data to provide Fraud Detect Services to other Fraud Detect Services customers, First Data will not identify Company as the source of the Fraud Detect Data.

4.2 Company represents and warrants that it: (1) will comply with all applicable data protection, data security or data privacy laws and regulations and has the legal right to provide and make available Fraud Detect Data (including personally identifiable information and device data) to First Data for the purposes described in this Schedule and the Fraud Detect Privacy Statement; (2) will maintain and make available to its mobile app or website end-users notice required under applicable data protection, data security or data privacy laws, including in a privacy policy containing legally adequate disclosures about its use of the Fraud Detect Services, including any legally required description of the purposes for which First Data may collect, use, or share the Fraud Detect Data; (3) will obtain any necessary consents or permission from its mobile app or website end-users, or otherwise has the lawful authority to provide their Fraud Detect Data to First Data for use as described in this Schedule and the Fraud Detect Privacy Statement, including any required consent to carry out automated individual decision making; (4) will build appropriate features into its mobile app, website, materials, and/or systems to (a) to accept complaints or disputes regarding transactions that are blocked using the Fraud Detect Services and act upon such complaints or disputes in its reasonable discretion including, allowing consumers to obtain human intervention in any Fraud Detect Services decision, to express their point of view and to contest any decision made as a result of the Fraud Detect Services and (b) to comply with the requirements of this Schedule; and (5) will provide reasonable cooperation and assistance upon First Data's request to enable First Data to meet its legal and internal compliance obligations with respect to the Fraud Detect Data, including providing First Data with documentation establishing that Company has complied with the above obligations. Company is responsible for the accuracy, quality, and legality of the Fraud Detect Data it provides to First Data or enables First Data to collect under this Schedule.

4.3 Company acknowledges and agrees that the Software may automatically collect a variety of information from or about end-users' computers or mobile devices, such as geolocation data, information from which location may be inferred, and unique identifiers; and associate such information with the end-user's transaction and such other information as Company may provide First Data about the end-user. The information collected automatically may change from time to time at First Data's sole discretion. First Data's Fraud Detect Privacy Statement describes First Data's privacy practices in connection with the Fraud Detect Services. Company shall address the relevant portions of the Fraud Detect Privacy Statement in its own privacy statement.

4.4 If an individual submits a privacy inquiry regarding information First Data maintains about the individual, Company will direct the individual to contact First Data with the request and Company will reasonably assist First Data in responding to the inquiry.

5. **Fees**. The Company will pay First Data the fees described below (**Fraud Detect Fees**) for the Fraud Detect Services. The Fraud Detect Fees are in addition to the other fees charged to process Company's transactions under the Agreement.

Annual Number of Transactions	Fee[1]	Driver
A – B[1]	$_____	per Fraud Detect Transaction Event*
C – D[1]	$_____	per Fraud Detect Transaction Event*
E +[1]	$_____	per Fraud Detect Transaction Event*
Monthly Fee	$_____	per month
Monthly Managed Services Fee	$_____	per month
Implementation Fee	$_____	one-time

[1] *First Data will review the number of transactions that Company submits for processing with the Fraud Detect Services within 30 days of the end of each Service Year and will adjust the per transaction fee for the Fraud Detect Services according to this table. The effective date for any adjustments to the transaction fees for the Fraud Detect Services will be the first day of the following Service Year. Each recurring one-year period during the Term, beginning on the Effective Date, is a* ***Service Year****.*

*Except, deposit transactions and user registrations are non-billable Fraud Detect Transaction Events.

6. **General**. First Data and Company each represents and warrants it has corporate authority to execute this Schedule, creating legally enforceable obligations. This Schedule may be executed electronically and in any number of counterparts, each of which will be considered an original and all of which constitute the same instrument. Electronic or other copies of the executed Schedule are effective. The Agreement remains in effect as supplemented by this Schedule.

Exhibit A

Fraud Detect
Implementation Form

This Implementation Form is between the State of North Carolina (**Company**) and First Data Merchant Services LLC (**First Data**); and supplements the Fraud Detect Schedule between the parties. Capitalized or other defined terms used, but not defined in this Implementation Form, have the meanings given to them in the Agreement or Schedule.

1 **Purpose**. The purpose of this Implementation Form is to describe the scope of Fraud Detect Services First Data will provide to Company and the Fraud Detect Services implementation requirements. First Data is only responsible for providing the Fraud Detect Services as described in this Implementation Form. All other services are considered outside the scope of this Implementation Form.

2 **Scope**. The Fraud Detect Services will provide:

2.1 Supervised machine learning model, to score transactions as described in Section 2.5.

2.2 Real-time fraud rules engine.

2.3 Software for Company to provide Device Data Elements, unless Company indicates it has or will obtain device intelligence software from a provider other than First Data.

2.4 An automated Fraud Detect Response for each of the Fraud Detect Transaction Events types noted in Section 7 and Payment Methods noted in Section 6.9.

2.5 Access to the User Interface to review/resolve each Fraud Detect Response, and obtain analytics and reporting.

3 **Training**. Up to 40 hours of training and consulting on how to use the User Interface and Fraud Detect Services, to be used within the first 30 days following implementation (any hours in excess of 40 will be invoiced at First Data's standard hourly rate).

4 **Assumptions**

4.1 First Data's ability to implement and deliver the Fraud Detect Services is subject to, and dependent on, the assumptions listed below and Company timely performing its responsibilities. If any assumption proves to be incorrect or if any of Company's responsibilities is not timely performed, (a) First Data may make changes to this Implementation Form, including the scope of the Fraud Detect Services, and/or (b) First Data's ability to perform under this Implementation Form may be impacted, and First Data will have no liability for its delay or inability to perform under this Implementation Form.

4.2 Assumptions:

4.2.1 First Data will not be responsible for implementation delays caused by Company or Company's third party service providers.

4.2.2 All data, information, and materials Company provides or makes available to First Data will be accurate and complete.

4.2.3 First Data may rely on all data, information, decisions, and approvals provided by Company.

5 **Fraud Detect Services Implementation Management.** First Data's Implementation Manager will:

5.1 Manage and coordinate First Data personnel assigned to implementing the Fraud Detect Services for Company.

5.2 Act as First Data's point of contact for all implementation issues and the Change Process (defined below).

5.3 Together, with Company's Project Manager (defined in Section 6.2), establish an implementation project plan with targeted implementation events. The Change Process (described in Section 8) will be used if either party desires a change to the finalized implementation project plan.

5.4 Conduct status meetings with Company to review implementation progress, issues, and potential risks. Frequency of these meetings will be mutually agreed by Company and First Data.

6 **Company Responsibilities**. Company will:

6.1 Provide First Data with prompt, reasonable access to Company's personnel (including third party vendors, as applicable) as necessary for First Data to implement and provide the Fraud Detect Services.

6.2 Assign a primary contact for the implementation and on-going receipt of Fraud Detect Services (**Company's Project Manager**). Company's Project Manager will be responsible for managing and coordinating Company personnel as required to

implement Fraud Detect Services, and to act as Company's point of contact for any implementation or Fraud Detect Services use issues and the Change Process.

6.3 Provide Company infrastructure or related components as necessary for Company to implement and use the Fraud Detect Services.

6.4 Provide technical support for Company's implementation team, including Company's third party vendors, as applicable.

6.5 Promptly provide the Fraud Detect Data when requested by First Data.

6.6 Indicate if Company has obtained or will obtain device intelligence software from a source other than First Data.
____ Yes ____No

6.7 Indicate if Fraud Detect Responses will consist of:
____ Allow and Prevent, OR
____ Allow, Prevent and Review

6.8 Indicate which Payment Methods will be sent to the Fraud Detect Services:
____ Visa
____ MasterCard
____ Discover
____ American Express
____ Wallet Payments

6.9 Integrate to the following First Data gateways, as applicable:
____ First API
____ uCom
____ IPG

6.10 Provide contact information for Company employees who will need access to the User Interface:
_____.

7 Fraud Detect Transaction Events:

____ Pre Authorization Transaction (if selected, cannot select Post Authorization Transaction)
____ Post Authorization Transaction (if selected, cannot select Pre Authorization Transaction)
____ Purchase Transaction
____ Deposit Transaction
____ Card Registration
____ User Registration

8 Change Process. Except as set forth in Section 4.1, any changes to this Implementation Form must be in writing. First Data will not be obligated to perform tasks related to changes in schedule, scope, cost, or other obligations until Company and First Data agree in writing to the proposed change in a fully-executed project Change Request Form. The Change Request Form will be supplied by First Data's Implementation Manager. A completed Change Request Form will include a justification for the change, estimated cost, schedule, resource requirements, and an implementation analysis.

9 Acceptance Criteria. Fraud Detect Services will be deemed "accepted" and ready for production use once Company is able to do each of the following (**Acceptance Criteria**):

9.1 Validate that Fraud Detect Transaction Events (as requested above) are being received by the Fraud Detect Services for scoring.
9.2 Validate that Company can receive a Fraud Detect Response for Fraud Detect Transaction Events (as requested above).
9.3 Validate that Company's fraud rules have been deployed within the Fraud Detect Services.
9.4 Validate that Company's Payment Types (as requested above) are deployed within the Fraud Detect Services.
9.5 Access the User Interface of the Fraud Detect Services.
9.6 Action data within the User Interface of the Fraud Detect Services (e.g., allow a transaction within the User Interface).
9.7 Access Fraud Detect Services reports (via User Interface).

If the Fraud Detect Services fail to materially meet the Acceptance Criteria, Company shall notify First Data in writing within 5 days following the acceptance period specifying in reasonable detail in what respects the Fraud Detect Services have failed to meet the Acceptance Criteria. First Data will have a reasonable amount of time to remedy such failure. Company shall repeat the acceptance testing process until the Fraud Detect Services are accepted. Acceptance will be deemed to occur on the earlier of the date: (1) Company confirms in writing the Fraud Detect Services materially meet the Acceptance Criteria at the end of the acceptance testing

period, or (2) 5 business days following the end of the acceptance testing period, if Company does not notify First Data in writing within those 5 business days, specifying in reasonable detail in what respects the Fraud Detect Services have failed to materially meet the Acceptance Criteria.

10 **Term and Termination**. This Implementation Form begins on the date it is signed by First Data (this date, the **Effective Date**), and, unless terminated as permitted in this Section 10, continues in accordance with its terms until the Fraud Detect Services are accepted as described in Section 9. Each party may terminate this Implementation Form and the Schedule immediately if the other fails to cure any material breach of this Implementation Form within 30 days after receiving notice specifying the applicable breach.

11 **General**. First Data and Company each represents and warrants it has corporate authority to execute this Implementation Form, creating legally enforceable obligations. This Implementation Form may be executed electronically and in any number of counterparts, each of which will be considered an original and all of which constitute the same instrument. Electronic or other copies of the executed Implementation Form are effective. The Schedule and Agreement remain in effect as supplemented by this Implementation Form.

[*signatures are on the next page*]