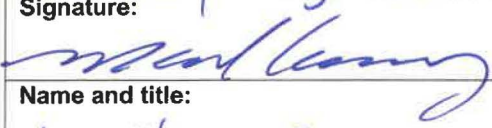


Giact Services Schedule



Giact Services Schedule version: 3.4 (08.14.2024)	Master Terms unique number: 1-32995164376
Client number: A-10072231	Effective Date: The date of last signature of the parties
Client entity: Galveston County, Texas	Refinitiv entity: Giact Systems, LLC
Address: 722 Moody, 5th Floor, Galveston, TX, 77550-2318, US	Address: 700 Central Expressway S., Suite 300, Allen TX 75013
Email: mark.henry@co.galveston.tx.us	Email:
Signature: 	Signature:
Name and title: MARK HENRY, COUNTY JUDGE	Name and title:
Date of signature: 06/17/2025	Date of signature:

The entities signing above are bound by this Schedule (the "Giact Services Schedule") to the Master Terms referenced above and applicable Giact Order Form(s).

Giact Services Schedule Terms and Conditions

1. Services.

1.1 Services. Subject to and in accordance with the terms of this Schedule, Giact will provide to Client the Services beginning on the date on which Client's Services are activated by Giact and Client is provided with access credentials by Giact (the "**Services Commencement Date**"). Client understands and agrees that Giact is not obligated to provide any Services to Client until Giact has notified Client that Client's account has been approved and Giact has issued access credentials to Client. The Services provided under this Schedule will be used solely by the Client to perform Transactions for its own commercial use. Client may not use the Services for the benefit of any third party. Any attempt by Client to use the Services for, or on behalf of a third party, will immediately and automatically terminate this Schedule and all Order Forms and may result in additional charges to Client. For purposes of this Schedule and all applicable Order Forms, "**Transaction(s)**" means any verification or other transaction, completed or submitted by Client to Giact pursuant to an Order Form. Giact may disclose Transactions, Data and all other information to its data providers in order to perform the Services.

1.2 License Grant. Subject to and in accordance with the terms of this Schedule, Giact hereby grants to Client a nonexclusive, limited, royalty-free right to access and use the Services for its internal business purposes only. Client will not (and will not allow any third party to) (i) disassemble, reverse engineer, decompile or attempt to discover any source code or internal structure or underlying ideas or algorithms of the Services (except to the extent that applicable law prohibits reverse engineering restrictions) or any part thereof, (ii) modify, adapt, alter, create derivative works based upon, or translate the Services, or any part thereof, (iii) transfer, provide, rent, lease, lend, resell, distribute, sublicense, or use for timesharing or service bureau purposes or otherwise use or allow others to use the Services for the benefit of any third party, or (iv) except as expressly provided for in this Schedule or the Agreement, copy, install or use the Services on any of its computer systems, servers, or networks. All rights not expressly granted herein are reserved by Giact or its suppliers.

1.3 Services-Related Documents. The Parties agree that Client's application and its supporting documentation which is incorporated by reference as if fully set forth herein. Client will promptly update in writing any changes to any information Client has previously supplied.

1.4 FCRA-Related Products (Applicable to gVerify, gAuthenticate).

1.4.1 Permissible Purpose and Use. Client understands that if Client uses Services that are subject to the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA") and any applicable analogous state law, as well as any applicable regulations and administrative requirements thereunder, under the FCRA, Client can obtain a consumer report only if Client has a permissible purpose to obtain and use the report. Client certifies that the consumer reports provided by Giact may be requested and used only if the Client has a legitimate business need for the information in connection with a business transaction that is initiated by the consumer, or the Client obtains the express written authorization of the consumer to obtain the consumer report. Client certifies that it will request and use the consumer reports for no other purpose.

If gVerify is a selected Service, Client agrees that it will use the gVerify consumer report solely:

- To validate the existence of an account (as defined in 12 C.F.R. § 229.2(a)) (an "Account") and all associated data in determining whether to accept or decline a check or automated clearinghouse entry (each an "Item") as payment for goods or services;
- As a factor in verifying, authorizing or guaranteeing a payment;
- To cash an Item or provide cash back from a deposit or payment;
- To decide whether to forward an Item for collection or represent it electronically; or,
- To determine whether to allow the account or application to be enrolled for use in connection with future transactions by validating that the account exists and/or is in good standing.

If gAuthenticate is a selected Service, the combined gAuthenticate and gVerify response is considered a consumer report and Client agrees that it will use the resulting consumer report solely:

- To determine whether to accept or decline an Item as payment for goods or services by validating that the consumer presenting such Item is an authorized account holder, user, or signatory of the Account on which such Item is drawn;
- To determine whether to accept or decline an Item as payment for goods or services by validating that the company name associated with such Item is the company name of the Account on which such Item is drawn;
- To determine whether to accept or decline an Item as funding for an account by validating that the consumer is an authorized accountholder, user, or signatory of the account used or to be used in connection with funding;
- To determine whether to transfer funds by validating that the consumer is an authorized accountholder, user, or signatory of the Account used or to be used in connection with the transfer of funds; or,
- To determine whether to allow an account to be enrolled for use in connection with future transactions by validating that the consumer is an authorized accountholder, user, or signatory of the account.

Nothing in this Section 1.4.1 shall prevent Client from using the consumer report provided via gVerify independent of gAuthenticate if gAuthenticate is also a selected Service.

Client shall not refuse or decline an Item based solely on data integrity, informational or positive (pass) responses provided from gVerify or gAuthenticate as is further described in the Verification Services Back Office User Manual.

UNDER § 619 OF THE FCRA, ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18, UNITED STATES CODE, IMPRISONED FOR NOT MORE THAN 2 YEARS, OR BOTH.

1.4.2 Documentation of Permissible Purpose. Client certifies that it will rely upon, and retain pursuant to Section 4.1 and 5.1, the following documentation and/or authorization from consumers as evidence of the Client's permissible purpose (Client must check all that apply):

- ☒ Physical Check presented by Consumer
☒ Electronic Signature of Consumer
☒ Written Authorization from the Consumer (on Signed Application)
☐ Written Authorization (by Recorded Voice Authorization)

1.4.3 Notice of Adverse Action and Consumer Dispute Process. Client understands and agrees that under the FCRA, as a user of the consumer report, Client must provide notice of adverse action in compliance with § 615 of FCRA when the consumer report information provided by Giact serves as the basis for the Client's declination. The notice must include contact for Giact including Giact's toll free number 1-833-802-8092.

Should a consumer contact Giact in response to a notice of adverse action, Client acknowledges and agrees that Giact may be required to provide additional information regarding Client. If required under the FCRA or requested by a consumer for any reason, Client identifies the following information below to be provided by Giact. Should Client's information below change, Client will notify Giact in writing promptly:

(Must be completed by Client)

Trade name (written in full) under which Client conducts business: Galveston County, Texas

Address: 722 Moody, 5th Floor, Galveston, TX 77550

Phone: 409-762-8621

1.4.4 Notice to Users. Client acknowledges receipt of the Notice to Users of Consumer Reports attached as Exhibit 1 to this Schedule and provided at: <https://www.giact.com/wp-content/uploads/2018/04/FCRANoticeToUsers.pdf>

1.5 Open Banking Services (Account Verification, Account Ownership Authentication, Account Balance). Client understands that if Client uses the following Open Banking Services: Account Verification, Account Ownership Authentication, Account Balance, Client will comply with the following:

1.5.1 Users. Client shall not allow a person to be a User unless such person has: (a) agreed to the terms and conditions presented by Finicity, a Mastercard company ("Finicity Ts&Cs"); (b) provided Explicit Consent to be legally bound by the Finicity T&Cs; and (c) been properly notified and provided Explicit Consent to Client consenting to Client's specific business purpose for which the Personally Identifiable Information is collected. "User" means any Client customer.

"Explicit Consent" means an electronic communication with a person that: (a) provides sufficient notice to such person regarding how User Data (as defined below) associated with that person will be used, including access, usage, storage, retention, and disposal of such person's User Data (including any use of anonymized data derived from the User Data) and the process for the revocation of consent (which process shall enable a person to readily revoke such consent); and (b) obtains from such person permission for a specific action that is maintained in a system log or database that ensures completeness, and integrity and permits verification of the consent upon request of the records. Explicit Consent must be consistent with standards developed for the collection of consent by the Financial Data Exchange (or subsequent industry organization) and at a minimum must be presented and captured in a clear and conspicuous manner and may not include a technology solution or script that automatically enrolls a person into an agreement without taking an express, recordable action.

1.5.2 Client Use of Data. Client shall not use or disclose User Data or Registration Data for any purpose that is not expressly permitted under this Agreement or by the User's Explicit Consent. Without limiting the foregoing, Client shall not sell, license, transfer, or otherwise disclose the User Data or Registration Data to any other party. Except as required by Applicable Law or to provide Services pursuant to the applicable Order Form and Schedule, the Parties agree that User Data and Registration Data retained by Giact's data provider(s) shall be in aggregated or anonymized form only and that Client shall not have the right to request (nor shall Giact's data provider(s) have the obligation to deliver) any User Data or Registration Data from Giact or its data provider(s) following termination of the applicable Order Form.

"User Data" means data pertaining to a User either provided to Client, Giact, and/or Giact's data provider(s) or obtained by Giact and/or Giact's data provider(s) as part of the Services provided to Client, including Personally Identifying Information.

"Registration Data" means User account access information and registration information as provided by Users to Client or Giact's data provider(s) for the purpose of accessing User Data from a financial institution that possesses account information regarding a User ("Provider"). Registration Data may also include Personally Identifiable Information.

1.5.3 Client & User Restrictions. Except as otherwise explicitly provided in the Agreement or as may be expressly required by Applicable Law, Client shall, and shall cause Users to: (a) use and grant access to the Services Technology only pursuant to the Agreement; (b) not attempt to gain unauthorized access to the Services Technology or their related systems or networks; (c) not access and/or engage in any use of the Services Technology in a manner that abuses or materially disrupts Giact's or Giact's data provider(s) networks, security systems, and/or websites; (d) not interfere with or disrupt the integrity or performance of the Services Technology or third-party data contained therein; (e) not access or use the Services Technology in any manner or for any purpose that infringes, misappropriates or otherwise violates any Intellectual Property Rights or other right of any third party; (f) not access or use the Services Technology for purposes of competitive analysis of the Services Technology, the development, provision or use of a competing software service or product or any other purpose that is to Giact's or Giact's data provider(s)'s detriment or commercial disadvantage, except as explicitly permitted by Giact or Giact's data provider(s) in writing; (g) not use the Services Technology for fraudulent purposes or otherwise in violation of Applicable Law; (h) except for Users saving their own User credentials or as required by applicable laws and only for so long as required, not retain, save or otherwise maintain any User credentials or other Personally Identifiable Information that could be used to access such User's financial information and other data; and (i) not use any "screen scraping" process(es) to obtain User Data directly or indirectly from any of Provider from which Giact's data provider(s) obtains User Data on behalf of User through the use of Registration Data (and not APIs or data feeds provided by or on behalf of Giact or Giact's data provider(s) as part of the Services Technology). If Client becomes aware of any activity prohibited by this section, Client shall, and shall cause Users to, immediately: (x) take all reasonable and lawful measures within their respective control that are necessary to stop the activity and to mitigate its effects (including, where applicable, by discontinuing and preventing any unauthorized access to the Services Technology); and (y) notify Giact of any such actual or threatened activity.

"Services Technology" means all of the following: (a) the Services and the equipment, interfaces, and all software and administrative platforms necessary to provide the Services; (b) any data or materials provided by or on behalf of Giact's data provider(s) or Giact on behalf of data provider(s) to Client, other than User Data, and (c) any and all technology, information, data, know-how, ideas, designs, software, inventions, documentation, resources and all other tangible and intangible items included therein and as provided to Client by Giact's data provider(s) or Giact on behalf of Giact's data provider, made, conceived, or received or reduced to practice by Giact's data provider(s), excluding Client's technology. Client shall not refer to Giact's data provider(s) directly or indirectly in any advertisement, news release, or publication without Giact's data provider(s)'s prior approval.

1.6 Non-FCRA-Related Services. Client certifies that because the information provided in the gAuth-only, ESI, gIdentify, CustomerID, gOFAC, gOFAC Monitoring, SecureLink, gScan, Beneficial ID, Giact Account Insights, and Open Banking: Account Verification, Account Ownership Authentication, and Account Balance Services is not consumer report information, Client will not request or use these Services as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes, tenant screening, or for any other purpose authorized under the FCRA or similar state or local statute, rules or regulations.

1.7 Gramm-Leach-Bliley Act ("GLBA")-Related Products (gIdentify Consumer, CustomerID, gAuth-only, Giact Account Insights).

1.7.1 Permissible Use of gIdentify Consumer, CustomerID, and Giact Account Insights. Client certifies that it will order and use gIdentify Consumer and CustomerID reports and Giact Account Insights information in connection with the following use involving the subject of the report and for no other use: To use in the ordinary course of business to verify the accuracy of information submitted by the consumer to protect against or prevent actual fraud, unauthorized transactions, claims or other liability. Client further understands and agrees that (i) Giact Account Insights is provided by GIACT and accessible by Client solely as an add-on Service to gVerify and/or gVerify Basic, and (ii) because Giact Account Insights is aggregated, historical information, it does not reflect a current status or the validity of an account.

1.7.2 Permissible Uses of gAuth-only. Client certifies that it will order and use gAuth-only reports in connection with verifying the accuracy of information submitted by the consumer to protect against or prevent actual fraud, unauthorized transactions, claims or other liability specifically for the following uses and for no other uses:

- To determine whether to accept or decline an Item as payment for goods or services by validating that the consumer presenting such Item is an authorized accountholder, user, or signatory of the Account on which the Item is drawn;
- To determine whether to accept or decline an Item as payment for goods or services by validating that the company name associated with such Item is the company name of the Account on which such Item is drawn;
- To determine whether to accept or decline an Item as funding for an Account by validating that the consumer is an authorized accountholder, user, or signatory of the Account used or to be used in connection with the funding;
- To determine whether to transfer funds by validating that the consumer is an authorized accountholder, user, or signatory of the Account used or to be used in connection with the transfer of funds;
- To determine whether to allow the Account to be enrolled for use in the connection with future transactions by validating that: (a) the consumer is an authorized accountholder, user, or signatory of the Account; or (b) the company name is associated with the Account.

1.7.3 Limited Access Death Master File gIdentify Indicator:

1.7.3.1 Client certifies that access to the death indicator provided by gIdentify and derived from the Limited Access Death Master File ("LADMF") is appropriate because Client (a) has (i) a legitimate fraud prevention interest, or (ii) a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty, (b) has systems facilities, and procedures in place to safeguard such information, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements reasonably similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986, and (c) agrees to satisfy such similar requirements.

1.7.3.2 Client further certifies that with respect to LADMF of any deceased individual at any time during the three calendar-year period beginning on the date of the individual's death, which is received by Client, Client shall not: (i) disclose any information contained on the LADMF with respect to any deceased individual to any person other than a person who meets the requirements of each of (a), (b), and (c) in Section 1.7.3.1; (ii) disclose any information contained on the LADMF with respect to any deceased individual to any person who uses the information for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty; (iii) disclose any information contained on the LADMF with respect to any deceased individual to any person who further discloses the information to any person other than a person who meets the requirements of each of (a) and (b) in Section 1.7.3.1; or (iv) use any information contained on the LADMF with respect to any deceased individual for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation or fiduciary duty.

1.7.3.3 Client agrees that it will immediately notify GIACT in writing if its status changes such that it would no longer have a permissible purpose to access LADMF and the circumstances of its change in status, and that it shall immediately cease ordering and accessing the LADMF.

1.7.3.4 Client shall not take any adverse action against any consumer without further investigation to verify the information from the LADMF.

1.7.3.5 Client shall have and maintain at all times that it is in possession of LADMF:

- (i) systems, facilities, and procedures in place to safeguard LADMF, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986, and agrees to satisfy the requirements of section 6103(p)(4) as if such section applied to Client.
- (ii) security provisions to protect the LADMF from being visible, searchable, harvestable or in any way discoverable on the World Wide Web.

1.7.3.6 Client understands that any successful attempt by any person to gain unauthorized access to or use of the LADMF that GIACT may immediately terminate Client's access to LADMF. In addition, any successful attempt by any person to gain unauthorized access may under certain circumstances may result in penalties as prescribed in 15 CFR § 1110.200 levied on Client and the person attempting such access. Client will take appropriate action to ensure that all persons accessing the LADMF through it are aware of their potential liability for misuse and/or penalties for attempting to gain unauthorized access. Any such access or attempted access is a breach, or attempted breach, of security, and Client must immediately report the same to GIACT and the National Technical Information Service ("NTIS") at LADMFcert@ntis.gov.

1.7.3.7 Client agrees to be subject to audit by GIAC and/or NTIS to determine Client's compliance with the requirements of the Agreement and 15 CFR Part 1110. Client agrees to retain a list of all employees, contractors, and subcontractors to which it provides LADM and to make that list available to NTIS and/or GIAC as part of any audits conducted hereunder. Client will not resell or otherwise redistribute the LADM.

1.7.3.8 Client shall comply with the requirements of 15 CFR Part 1110, as though set forth in full herein. Client may not resell or otherwise distribute the LADM. Client acknowledges that its access and use of LADM is governed by federal law and venue for any claims is in the federal courts. Client failure to comply with laws related to access and use LADM may subject Client to criminal and civil penalties.

1.7.3.9 Should Client cease to have access rights to LADM or upon termination of the Services Agreement for any reason, Client shall destroy all LADM and will certify to GIAC in writing that it has destroyed all such LADM.

1.7.3.10 GIAC, and its data suppliers (including government agencies) (a) makes no warranty, express, implied or statutory, and specifically disclaims all warranties, with respect to the LADM, including but not limited to, implied warranties of merchantability and fitness for any particular use or that use of the LADM constitutes compliance with any law or regulation; (b) assume no liability for any direct, indirect or consequential damages flowing from any use of any part of the LADM, including infringement of third party intellectual property or privacy rights; and (c) assume no liability for any errors or omissions in the LADM. The LADM contains inaccuracies. As such, neither GIAC, NTIS, nor the Social Security Administration which provides the LADM to NTIS, guarantees the accuracy of the LADM. The LADM does not contain death records for all deceased persons. Therefore, the absence of a particular person in the LADM is not proof that the individual is alive. Further, it is possible for the records of a person who is not deceased to be included erroneously in the LADM. Client acknowledges and agrees that the LADM does not guarantee the identity of or information regarding any individual and that Client has processes in place to independently verify the information provided in the LADM.

1.7.3.11 In addition to Client's indemnification obligation stated elsewhere in the Agreement, Client shall indemnify and hold harmless GIAC and its data suppliers (including government agencies) from all claims, liabilities, fines, assessments, demands, damages, expenses, and losses arising from or in connection with the use of the LADM by or through Client.

1.7.3.12 Client agrees that it will provide a renewal certification no less than every three years.

1.7.3.13 The terms and condition of this Section 1.7.3 shall survive termination of the Agreement for any reason for as long as the LADM is in Client's possession or control.

1.7.3.14 Client acknowledges that the terms of this Section 1.7.3, in the event of conflict with the terms of the Agreement, apply in addition to, and not in lieu of, such terms in the Agreement with respect to the LADM only.

1.8 gIDENTIFY Business with IRS TIN Validation Data. By using the gIDENTIFY Business with IRS TIN Validation data, Client appoints GIAC's Third Party Provider as proxy to perform tax identification number (TIN) verification with the Internal Revenue Service (IRS).

1.8.1 Client certifies it will only forward TIN matching requests for itself and has filed or is likely to file forms 1099-B, DIV, INT, K, MISC, OID or PATR in the past and that any TIN/names being checked relate to an account(s) where a reportable payment subject to backup withholding is made or is likely to be made as defined under §3406(b)(1) of the Internal Revenue Code.

1.8.2 Client agrees to:

- (i) Comply with all requirements of revenue procedure 2003-9;
- (ii) Transmit only name/TIN combinations relating to accounts with respect to which a reportable payment is made, or is likely to be made, on or after the effective date of revenue procedure 2003-9; and
- (iii) Maintain the confidentiality of information obtained through TIN solicitation activities in accordance with the requirements of §31.3406(f)-1 of the Employment Tax Regulations.

1.8.3 Client further certifies that it is either an "Authorized Agent" or "Delegated User" as defined by the IRS in the TIN Matching Revenue Procedure to collect and match TINs, names, and/or name controls on behalf of the Client and appoints GIAC's Third Party Provider as proxy with respect to this procedure.

1.9 gOFAC and gOFAC Monitoring. gOFAC is an information service that is based on information that was not collected, in whole or in part, for the purpose of serving as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; employment purposes; or any other purpose authorized under the FCRA. Accordingly, Client certifies it will not use any information provided through gOFAC or gOFAC Monitoring as part of its decision-making process for determining the consumer's eligibility for any credit products or other products, benefits, or services applied for. Client acknowledges that such an indicator is merely a message that the consumer may be listed on one or more U.S. government-maintained lists of persons subject to economic sanctions, and Client further certifies that upon receipt of a gOFAC alert, it will contact the appropriate government agency for confirmation and instructions. The gOFAC alert indicator may or may not apply to the consumer whose eligibility is being considered by Client. Client acknowledges and agrees that the gOFAC service, the gIdentify Consumer Standard service, and the gIdentify Business Standard service must be enabled and one of those services must be first utilized for all consumers or entities at the stated rate set forth on the applicable Order Form before any such consumers or entities will be subject to gOFAC Monitoring; provided, however, that if Client utilizes the gIdentify Consumer Standard and gIdentify Business Standard services, Client is not required to also first utilize the gOFAC service to access the gOFAC Monitoring service. Client further understands that the gOFAC Monitoring service, if enabled, will automatically be triggered for all consumers and entities submitted by Client in connection with a gOFAC, gIdentify Consumer and/or gIdentify Business Transaction, and each such consumer and entity will thereafter be

monitored via the gOFAC Monitoring service until Client manually removes such person or entity from Client's monitoring list and Client will be charged on a monthly basis per each consumer and entity monitored at the rate set forth on page 1 of this Agreement. Client understands and agrees that information provided to Client via gOFAC Monitoring will be provided to Client via the following email address designated by Client:

Non-personalized, consistently monitored email address for Client's receipt of gOFAC Monitoring information: _____

Should Client change the above email address, Client agrees to provide notification in writing of any such change at least five (5) business days in advance.

1.10 gIdentify Persistent Monitoring. Client understands and agrees that it shall first submit to the gIdentify Consumer Standard service, at the rates set forth on the applicable Order Form, all consumers it seeks to place under the gIdentify Persistent Monitoring service. Client further understands that it shall be required to assign a unique identifier that complies with Giact's requirements to each consumer placed under the gIdentify Persistent Monitoring service and supply such unique identifier to Giact. Client further understands that the gIdentify Persistent Monitoring service, if enabled, will automatically be triggered for all consumers to which a unique identifier is assigned by Client and which relate to a recognized identity profile, and each such consumer will thereafter be placed under the gIdentify Persistent Monitoring service until Client manually removes such person from Client's gIdentify Persistent Monitoring service. Client understands that the gIdentify Persistent Monitoring service will trigger an alert to Client whenever information about a consumer to which Client has assigned a unique identifier has changed. To obtain new information regarding the consumer, Client must inquire about the consumer via the gIdentify service at the Rate/Transaction set forth on the applicable Order Form. Client understands and agrees that information provided to Client via gIdentify Persistent Monitoring will be provided to Client via the following email address designated by Client: _____

Non-personalized, consistently monitored email address for Client's receipt of gIdentify Persistent Monitoring information (which may not be the same email address used for gOFAC Monitoring):

Should Client change the above email address, Client agrees to provide notification in writing of any such change at least five (5) business days in advance. Notwithstanding Client's provision of the above email address to Giact, Client understands and agrees that Client is responsible for consistently and regularly checking in Client's Giact back office and/or through an API inquiry for the existence of any gIdentify Persistent Monitoring alerts.

1.11 Declination. Giact reserves the right to decline to provide the Services or terminate the applicable Order Form immediately (a) as required by a data provider, financial institution, or Applicable Law and as required by judicial or other governmental demand, order, subpoena, or law enforcement request, (b) if Giact or Giact's data provider(s) reasonably determines the provision or consumption, as applicable, of all or any portion of the Services may pose a material adverse risk to Giact's or Giact's data provider(s)'s brand or reputation, and such risk cannot be remediated by the commercially reasonable efforts of that Party, or (c) if it reasonably believes that (x) Client is using or may use the Nonpublic Personal Information (as that term is defined in 12 C.F.R. § 1016.3(p)(1)) ("Data") or the Services for a purpose other than as permissible under the Agreement or in violation of Applicable Law, (y) Client has failed to comply with any term of the Agreement, or (z) Client or User has been, or is likely to be involved in any fraudulent, misleading, or unlawful activities relating to or in connection with the Services. For purposes of this Schedule, "Applicable Law(s)" means laws, policies, guidelines, regulations, ordinances, and rules applicable to a Party, this Schedule, its business or the Transactions and the orders of any governmental authority or regulatory body having jurisdiction over the subject matter hereof, including, but without limitation, the rules promulgated by industry associations, the U.S. Federal Trade Commission, the electronic communication rules of the CAN-SPAM Act, the FCRA, the GLBA, including its privacy and data security requirements and the unfair, deceptive, or abusive acts or practices requirements and regulations thereof, applicable bank secrecy and outsourcing requirements, applicable privacy and data security laws and regulations, the Foreign Corrupt Practices Act, the UK Bribery Act, and all other applicable anti-corruption and anti-bribery laws, the Driver's Privacy Protection Act, and the Telephone Consumer Protection Act, the Restore Online Shoppers' Confidence Act, the General Data Protection Regulation, and regulations and equivalent state laws thereof.

2. Security.

2.1 Access to Account; ID and Passwords. Client will set up an account ID and password in order to obtain secured access to the Services. Client will only grant access to its account ID and password to its employees who need access in order for Client to conduct its business. Client will be solely responsible for maintaining adequate security and control of its account ID and password (or any other codes for purposes of providing Client access to the Services). Giact will be entitled to rely on information it receives from Client through the secured access and may assume that all such information was transmitted by a Client employee. Client will comply with all Giact recommendations and notices regarding the security of Client's account ID, password and Giact account(s).

2.2 Security Requirements. Client will establish and maintain such security and privacy measures and procedures as are required by Applicable Laws and that which are reasonably practicable to provide for the safe custody, control and access of any (i) Data, and (ii) Giact's Confidential Information in its possession and to prevent unauthorized access thereto or use thereof.

3. Data Security and Retention.

3.1 Data Security. Each Party will be solely responsible for the security of the Data residing on its servers (or third-party servers designated by such Party). Each Party will comply with all Applicable Laws governing the security, collection, retention and use by it of financial information (including checking account numbers, and all other personally identifiable customer information). Client agrees to provide notice to its customers by all appropriate means, including but not limited to, by providing information on its web site that discloses how and why personal and financial information is collected and used, including uses governed by this Schedule. Client agrees that it is solely responsible for verifying the accuracy and completeness of all Transactions submitted to Giact associated with Client's use of the Services.

3.2 Industry Standards. Each Party will comply with all then-current legal obligations and industry standard security measures, as applicable, including but without limitation those issued by industry associations and the Federal Trade Commission, associated with the collection, security, dissemination and destruction of Data and Transaction data. Each Party warrants that it has taken precautions as are necessary to ensure that its server and electronic systems are secure from breach or intrusion by unauthorized third parties. In the event that a Party's system is breached, and an unauthorized third party has access to or has accessed Data or Transaction data, the breached Party will notify the other Party promptly in writing of the breach and will, at its own expense, take all measures necessary to remediate the breach, including notifying customers (as necessary), and take precautions to prevent future systems and data breaches.

3.3 Data Retention. Client will compile and retain permanent records of all Transactions and Data for Client's reference. Except as otherwise provided herein, at no time will Giact have an obligation to store, retain, report or otherwise provide any copies of or access to any records of Transactions or Data collected or processed by Giact.

4. Representations and Warranties. Giact and Client represent and warrant, as applicable, as follows:

4.1 Authorized Use of Data. Client (including its employees or agents) (i) has obtained all required approvals from its customers relating to the Services, and (ii) will maintain proof of all such approvals and provide such proof to Giact at Giact's request. If Beneficial ID is an included Service and Client is required by law to obtain consent from persons supplying information in response to a request from Client, Client will supply legally compliant consent language to Giact. Should persons supplying information in response to a request from Client withdraw consent, Client shall notify Giact of such withdrawal of consent at support@giact.com immediately.

4.2 Compliance with Law and Guidelines. Each Party will comply, at its own expense, with all Applicable Laws. In addition, Client warrants and represents that it will comply with all the current policies, procedures and guidelines of Giact set forth in this Schedule, and the Permissible Purpose and use herein, as may be amended by Giact from time to time upon 30 days written notice to Client.

4.3 Accuracy of Client's Representations. All representations and statements made, and information supplied by Client in this Schedule, or in any other document relating hereto by Client or on Client's behalf, including the Application and any supporting documentation, are true, accurate and complete in all material respects and will continue to be true, accurate and complete throughout the Term. Client hereby authorizes Giact to investigate and confirm the information submitted by Client herein and to perform periodic reviews during the Term. For this purpose, Giact may utilize consumer reporting agencies, its own agents and all other legal means.

4.4 No Marketing Use. Client certifies that it will not use the Services for any marketing purposes, including but not limited to creating a telemarketing call list or direct mailing list.

4.5 Use of Data in U.S. Client affirms and agrees that it will not transfer, process, store, or access any Services or other information or responses provided by Giact in connection with the Services outside of the United States without Giact's written consent. With the exception of the gIdentify Global, EPIC World-Check, and gOFAC services, Client further affirms and agrees that it will not submit to Giact any Data regarding non-U.S. residents.

4.6 Governmental Request for Personally Identifiable Information. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Client will promptly inform Giact, in each case in writing in accordance with the notice provision set forth in the Agreement, if any competent authority, regulator or public authority with jurisdiction requests disclosure of, or information about, Personally Identifiable Information that are processed in connection with the Services. Client will, without limiting its rights under Applicable Law, cooperate with Giact as reasonably necessary to comply with any direction or ruling related to the Services made by such authorities.

5. Review and Audit Rights.

5.1 Audit of Client. During the Term and for a period of two years thereafter, Giact and/or its data provider(s) will have the right to conduct an audit of Client's use of the Services and Data during normal business hours and no more than once each calendar year upon reasonable notice to Client, and additionally if at any time Giact and/or its data provider(s) has a reasonable basis to believe that Client is not in compliance with the terms and conditions of this Schedule. Client agrees to provide all reasonable assistance with audits and comply with all reasonable requests by Giact and/or its data provider(s) in its efforts to verify Client's compliance with this Schedule. Giact will not request access to any books, records, information or processes not directly related to the Services or Data.

5.2 Non-Compliance with Audits. If an audit reveals that Client is not in compliance with this Agreement Schedule or Applicable Law or if compliance cannot be verified, Giact may immediately suspend Client's access to the Services and Data and the Parties will create a relevant plan to cure Client's non-compliance. Once a plan has been created and a resolution period established, Client must provide written certification to Giact and/or its data provider(s) that all conditions of the plan are complete before the expiration of the resolution period. If the plan is not completed in a timely manner, Giact may terminate this Schedule on written notice to Client. Nothing in this Section will be construed to limit any of Giact's other rights or remedies under the Agreement or this Schedule.

6. Priorities

6.1 In the event of any conflict between:

6.1.1 the Order Form for Giact Services and this Schedule, the Order Form shall prevail;

6.1.2 the Master Terms and this Schedule, this Schedule shall prevail; and

6.1.3 a Schedule to the Master Terms and this Schedule, this Schedule shall prevail.

7. Disclaimers

7.1 Client understands, acknowledges and agrees that except as otherwise provided herein, the Services are provided to Client "as is" and neither the Services nor any other technology, content, intellectual property, nor any other information, data, products, or services, will be available, accessible, uninterrupted, timely, secure, accurate, complete, or error-free.

7.2 Client understands and agrees that it is solely responsible for any decisions it makes or actions it takes in connection with information provided by the Services.

EXHIBIT 1

All users of consumer reports must comply with all applicable regulations. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

NOTICE TO USERS OF CONSUMER REPORTS: OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681–1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau's (CFPB) website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the CFPB's website. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.**

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are:

- As ordered by a court or a federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5)

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of "prescreened" information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(f) prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term “adverse action” is defined very broadly by Section 603. “Adverse actions” include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA—such as denying or canceling credit or insurance or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained from Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained from Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

D. Users Have Obligations When Fraud and Active Duty Military Alerts Are in Files

When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of the reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the address in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed. Federal regulations are available at <http://www.consumerfinance.gov/learnmore>.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. Federal regulations have been issued that cover disposal.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulations prescribed by the CFPB.

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) ("Notice to the Home Loan Applicant").

III. OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry

If information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.
- **Before** taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer's rights. (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken.

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2)

The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subjects of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure described below.
- Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its agent complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes - or in connection with a credit transaction (except as provided in federal regulations) - the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(l), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain preestablished criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.

- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.
- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

In addition, the CFPB has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The relevant regulation is 12 CFR 1022.54.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:

(1) the identity of all end-users;

(2) certifications from all users of each purpose for which reports will be used; and

(3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part, and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619.

The CFPB's website, www.consumerfinance.gov/learnmore, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:

Section 602	15 U.S.C. 1681
Section 603	15 U.S.C. 1681a
Section 604	15 U.S.C. 1681b
Section 605	15 U.S.C. 1681c
Section 605A	15 U.S.C. 1681cA
Section 605B	15 U.S.C. 1681cB
Section 606	15 U.S.C. 1681d
Section 607	15 U.S.C. 1681e
Section 608	15 U.S.C. 1681f
Section 609	15 U.S.C. 1681g
Section 610	15 U.S.C. 1681h
Section 611	15 U.S.C. 1681i
Section 612	15 U.S.C. 1681j
Section 613	15 U.S.C. 1681k
Section 614	15 U.S.C. 1681l

Section 615	15 U.S.C. 1681m
Section 616	15 U.S.C. 1681n
Section 617	15 U.S.C. 1681o
Section 618	15 U.S.C. 1681p
Section 619	15 U.S.C. 1681q
Section 620	15 U.S.C. 1681r
Section 621	15 U.S.C. 1681s
Section 622	15 U.S.C. 1681s-1
Section 623	15 U.S.C. 1681s-2
Section 624	15 U.S.C. 1681t
Section 625	15 U.S.C. 1681u
Section 626	15 U.S.C. 1681v
Section 627	15 U.S.C. 1681w
Section 628	15 U.S.C. 1681x
Section 629	15 U.S.C. 1681y