

MASTER SERVICES AGREEMENT

This Master Services Agreement ("Agreement") is entered into between Sontiq, Inc. dba CyberScout, a Delaware corporation with its principal offices located at 9920 Franklin Square Drive, Unit 250, Nottingham, MD 21236 ("CyberScout"), and Constangy, Brooks, Smith & Prophete, LLP ("Law Firm") located at 600 Stewart Street Suites 300 & 400 Seattle, Washington 98101, who hereby engages CyberScout on behalf of Law Firm's client as identified below ("Company"), effective as of the date indicated below ("Effective Date"). CyberScout and Company each may be referred to as a "Party" and collectively as the "Parties."

Rains County Texas

Name of Company

**167 E. Quitman St.
Emory, TX 75440**

Principal Office Address

9/12/2025

Effective Date

NOW, THEREFORE, in consideration of the mutual terms, provisions, covenants, conditions, understandings, and agreements herein, the receipt and sufficiency of which is acknowledged, the Parties agree as follows:

1. PROVISION OF SERVICES

During the term of this Agreement, CyberScout shall provide each service as described separately in each statement of work ("SOW") mutually agreed to by the Parties (the "Services"). Each executed SOW shall be attached hereto and is incorporated by reference. CyberScout shall provide the Services to Company solely for the benefit of Company's Customers as defined or identified in the applicable SOW and shall have no contractual obligations to the Customer unless a Customer has separately contracted with CyberScout.

2. FEES AND PAYMENT

Company agrees to pay CyberScout the fees applicable to each SOW as set forth in the executed SOW. Company will be responsible for all taxes, fees or charges levied or assessed by any governmental authority or agency based upon the charges under this Agreement or the Services, except taxes levied or assessed on the net income or profit of CyberScout, if any. Company shall be solely responsible for all financial obligations to CyberScout in connection with this Agreement.

3. TERM AND TERMINATION

3.1 Term. The Agreement will begin on the Effective Date and will continue in effect until otherwise terminated in accordance with Section 3.2 below.

3.2 Termination. Either Party may terminate this Agreement and any SOW: (a) immediately in the event of a material breach of this Agreement or any such SOW by the other Party that is not cured within thirty days of written notice by the

other Party specifying the default (or, in the case of Company's failure to pay any amount due, within ten days of written notice); or (b) immediately in the event of the other Party's bankruptcy, insolvency, liquidation, or cessation of business. Either Party may also terminate this Agreement upon thirty days' written notice to the other Party for any reason if there are no SOWs then currently in effect. Upon termination of this Agreement for any reason, all outstanding SOWs shall immediately terminate. Except as expressly provided herein, termination of this Agreement or any SOW is a nonexclusive remedy for breach. All rights and obligations accrued prior to termination will survive termination.

3.3 Post-Termination Obligations. Upon termination or expiration of this Agreement and all SOWs, CyberScout and Company will each, within thirty days, return to the other party or destroy all copies of the other's Confidential Information and will certify, in writing, delivery or destruction of all such Confidential Information and copies thereof. However, a party shall not be required to search for information stored in backup tapes or similar backup media if the information will be destroyed in the ordinary course pursuant to a commercially reasonable schedule and any such stored information is treated as Confidential Information until it is destroyed.

4. CONFIDENTIALITY

4.1 Confidential Information. Each Party will regard any information provided to it by the other Party and designated in writing as proprietary or confidential to be confidential ("Confidential Information"). Confidential Information shall also include information that would otherwise be understood by a reasonable person to be confidential or proprietary given the nature of the information and/or the manner in which it is disclosed. The receiving Party shall not disclose Confidential Information to any person or entity *except* to a director, officer, employee, outside consultant, third party service provider, or advisor (collectively "Representatives") who have a need to know such Confidential Information in the course of their duties for the receiving Party and who are bound by a duty of confidentiality no less protective of the disclosing Party's Confidential Information than this Agreement. The receiving Party and its Representatives shall use such Confidential Information only for the purpose for which it was disclosed and shall not use or exploit such Confidential Information for its own benefit. Each Party accepts responsibility for the actions of its Representatives and shall protect the other Party's Confidential Information in the same manner as it protects its own valuable confidential information, but in no event shall less than reasonable care be used. The Parties agree that the terms and pricing of this Agreement are Confidential Information. A receiving Party shall promptly notify the disclosing Party upon becoming aware of a breach or threatened breach hereunder and shall cooperate with the disclosing Party in enforcing its rights.

4.2 Exclusions. Information will not be deemed Confidential Information hereunder if it: (i) is known prior to receipt from the disclosing Party, without any obligation of confidentiality;

(ii) becomes known to the receiving Party from a source other than one having an obligation of confidentiality to the disclosing Party; (iii) becomes publicly known or otherwise publicly available, except through a breach of this Agreement; or (iv) is independently developed by the receiving Party without use of the disclosing Party's Confidential Information. The receiving Party may disclose Confidential Information to the extent required by applicable law, legal process or government regulation, provided that it gives the disclosing Party reasonable prior written notice to permit the disclosing Party to contest such disclosure.

5. OWNERSHIP RIGHTS

5.1 Company. Company retains ownership of all right, title, and interest in any information, data, and materials provided by Company to CyberScout in connection with this Agreement ("Company Materials") and all of Company's logos and trademarks. Company hereby grants to CyberScout a limited, worldwide, non-exclusive, non-transferable (except as set forth in Section 11.2), right to use and display the Company Materials, logos and trademarks solely as necessary to provide the Services.

5.2 CyberScout. As between Company and CyberScout, all right, title, and interest in the Services and any trade secrets, know-how, processes, or works of authorship incorporated into the Services or otherwise made available to Company by CyberScout in the course of providing the Services ("CyberScout Materials") are and shall remain CyberScout's or its licensors'. The CyberScout name, all CyberScout logos, and the product names associated with the Services are trademarks of CyberScout or third parties, and no right or license is granted to use them.

5.3 Neither party shall take any action inconsistent with the other party's ownership of such other party's (or its licensors') logos and trademarks, and any benefits accruing from the use of a party's or its licensors' logos or trademarks shall automatically vest in the owner.

6. PERSONAL INFORMATION / DATA SECURITY

6.1 Compliance with Laws. Both parties agree to comply with all applicable laws and regulations regarding privacy and protection of personal information ("Privacy Laws"). If necessary to comply with Privacy Laws, CyberScout may suspend or cease providing Services and shall not be deemed to be in breach as a result.

6.2 Use of Information. CyberScout collects, stores and uses personal details of Customers in accordance with CyberScout's privacy notice that is located at cyberscout.com/privacy-policy, as amended from time to time. CyberScout assumes no responsibility for the use of any such information by any third party (such as a third-party supplier of credit or fraud monitoring products) if and to the extent the information is provided directly to the third party by a Customer.

6.3 Safeguarding Information Provided by Customer. CyberScout shall take commercially reasonable steps to safeguard non-public personal information provided by Customers to CyberScout, including encrypting with at least 128-bit encryption any such information that CyberScout stores electronically.

6.4 Breach Incident. CyberScout will promptly notify Company of any security breach that results in unauthorized intrusion of CyberScout's physical location or storage facilities, including computerized data storage facilities, that may affect Customers. Such notification shall include a summary of the intrusion, CyberScout's corrective action, and the information that may have been obtained. CyberScout and Company shall comply with any notification requirements under applicable law and cooperate with any law enforcement investigations.

7. REPRESENTATIONS AND WARRANTIES

7.1 CyberScout and Company each hereby represents to the other that this Agreement has been duly and validly executed and delivered by it and constitutes its legal, valid and binding obligation; and that its execution and performance of this Agreement does not violate or constitute a default under (i) any law, statute, ordinance, rule, regulation, judgment or decree applicable to it, or (ii) the terms of any other agreement, document or instrument applicable to it.

7.2 If Company is entering into this Agreement or any SOW on behalf of, or to procure services for, an affiliate or client of Company, Company represents and warrants that it has authority to do so and that Company's entry into the Agreement and/or SOW thereby binds such affiliate or client to the terms thereof.

8. INDEMNIFICATION ✱

8.1 Each Party (the "Indemnifying Party") will indemnify, defend, and hold harmless the other Party, its parents, subsidiaries, affiliates, directors, officers, employees, agents and subcontractors (any such Party seeking indemnification, the "Indemnified Party") from and against any bona fide legal claim against the Indemnified Party made by any Customer or other third party arising out of the gross negligence or willful misconduct of the Indemnifying Party in connection with this Agreement, any of which is hereinafter referred to as a "Claim."

8.2 The indemnification obligations under this Section 8 are subject to the Indemnified Party (i) promptly notifying the Indemnifying Party of the Claim, (ii) permitting the Indemnifying Party to assume sole control of the defense and settlement of such Claim (but the Indemnified Party will have the right to participate in the defense or settlement at its sole cost and expense), and (iii) providing the Indemnifying Party with all reasonable assistance in connection with defending or settling any such Claim. The Indemnifying Party shall not settle any Claim in a manner adverse to the Indemnified Party without the prior written approval of the Indemnified Party.

9. LIMITATION OF LIABILITY

9.1 Consequential Damage Exclusion. Neither Party shall be liable to the other or to any third party for loss of profits or for any special, indirect, incidental, consequential or punitive damages in connection with this Agreement, whether arising by statute, contract, tort, or otherwise, even if it is aware of the possibility of the occurrence of such damages.

9.2 Limitation of Liability. Except for a Party's breach of Section 4 or its willful misconduct, and excluding Company's payment obligations under this Agreement, the total cumulative liability of each Party for any and all claims and damages under this Agreement, whether arising by statute,

contract, tort or otherwise, will not exceed the fees paid by Company to CyberScout hereunder during the twelve (12) month period immediately preceding the event giving rise to the claim.

9.3 Nothing in this Section 9 is intended to limit a Party's liability for fraudulent conduct or for death or personal injury caused by its negligence.

10. DISCLAIMERS OF WARRANTIES

THE SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, CYBERSOUT EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. CYBERSOUT MAKES NO WARRANTY THAT (i) PAST IDENTITY FRAUD WILL BE RESOLVED, IN WHOLE OR IN PART, OR THAT (ii) FUTURE IDENTITY FRAUD WILL BE PREVENTED.

11. GENERAL

11.1 Entire Agreement. This Agreement contains the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior or contemporaneous proposals, representations, and communications (written or oral) between the Parties relating thereto.

11.2 Assignment. Company may not assign or delegate any of its rights or obligations under this Agreement without the written consent of CyberScout, which may not be unreasonably withheld. CyberScout may assign this Agreement and all SOWs as part of a corporate reorganization, consolidation, merger, or sale of all or substantially all of its assets, shares, or business to which this Agreement relates. Any attempted assignment or delegation that is not permitted by this Agreement will be void.

11.3 Affiliates; Subcontractors. CyberScout may in its discretion provide Services through one or more of its international Affiliates. "Affiliate" means a parent, sister, or subsidiary company. CyberScout may also utilize third-party subcontractors in its discretion to provide additional working capacity, availability, and/or specialized capabilities that may be called for under the circumstances. At all times, CyberScout shall remain responsible for all aspects of the Services. Company acknowledges that if the Services include a credit report and/or credit or identity monitoring, the monitoring is obtained from a third party vendor.

11.4 Continuation of Services. CyberScout may offer Customers the option to continue receiving Services (or similar services) at their own cost following the conclusion of Services under this Agreement. With respect to such follow-on services that a Customer may elect to receive at their own cost, the Customer will become a CyberScout customer pursuant to a separate agreement with CyberScout, and CyberScout shall have no reporting or other obligations to Company.

11.5 Relationship of the Parties. CyberScout and Company are independent contractors, and nothing in this Agreement shall be construed as making them partners or creating a relationship of employer and employee, master and servant, or principal and agent between them, for any purpose.

11.6 Notices. All notices provided for hereunder shall be in writing and shall be deemed given (i) when delivered on a business day if delivered personally during normal business hours at the place of receipt; (ii) on the next business day after deposit with any overnight courier for next business day delivery, if such date is a business day at the offices of the addressee; or (iii) the date of receipt if delivered by certified mail, return receipt requested, postage prepaid. "Business day" is defined as any day other than Saturdays, Sundays, and statutory holidays in the relevant jurisdiction. Notices shall be addressed as follows or to such other address as a Party may specify in accordance with this Section 11.6:

If to CyberScout:

Sontiq, Inc. dba CyberScout (Attn: Matt Cullina)
9920 Franklin Square Drive, Unit 250
Nottingham, MD 21236

**With a copy to:*

Sontiq, Inc. dba CyberScout (Attn: General Counsel)
9920 Franklin Square Drive, Unit 250
Nottingham, MD 21236

If to Company: To the attention of Company's signatory to this Agreement at the address set forth in the preamble above.

11.7 Governing Law and Dispute Resolution. This Agreement and any dispute or claim arising out of or in connection with its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of the State of Delaware without regard to its conflicts of laws provisions. The parties irrevocably consent to the exclusive jurisdiction and venue of the state or federal courts located in New Castle County, Delaware for all such disputes or claims.

11.8 Cooperation in the Event of Investigation. CyberScout agrees to assist and support Company in the event of an investigation by law enforcement or similar authorities, as such investigation relates to the services provided, or information collected or received, under this Agreement. Company will reimburse CyberScout for any reasonable, pre-approved out-of-pocket costs incurred in the course of complying with this section, but Company shall have no such reimbursement obligation if CyberScout or its actions are a principal subject of the investigation.

11.9 No Party shall be deemed to have waived any of its rights, powers or remedies hereunder, or to have waived any condition precedent, unless such waiver is embodied in a writing executed by such Party which explicitly sets forth the Party's intent to waive the matter in question.

11.10 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which, together, shall constitute one and the same instrument. Signatures to this Agreement or any SOW transmitted by facsimile, by electronic mail in "portable document format" (".pdf"), or by any other electronic means which preserves the original graphic and pictorial appearance of the Agreement, shall have the same effect as physical delivery of the paper document bearing the original signature and shall for all purposes be treated as original.

Executed and delivered by the parties' authorized representatives on the last date indicated below.

Constangy, Brooks, Smith & Prophete, LLP

Sontiq, Inc. dba CyberScout

Signature of Authorized Representative

Signature of Authorized Representative

Print Name of Signer

Print Name of Signer

Print Title of Signer

Print Title of Signer


Date Signed

Date Signed

CyberScout Use Only

Contract No:

Rains County Texas



Signature of Authorized Officer

Print Name of Signer **Brent D. Hilliard**

Print Title of Signer **County Judge**

10-10-2025

Date Signed

STATEMENT OF WORK FOR BREACH SERVICES

This statement of work, including all exhibits attached hereto (the "SOW"), is entered into between Sontiq, Inc. dba CyberScout, a Delaware corporation, with its principal offices at 9920 Franklin Square Drive, Unit 250, Nottingham, MD 21236 ("CyberScout"); and Constangy, Brooks, Smith & Prophete, LLP ("Law Firm") located at 600 Stewart Street Suites 300 & 400 Seattle, Washington 98101 ("Law Firm"), who hereby engages CyberScout on behalf of Law Firm's client as identified below ("Company"), effective as of the date indicated below ("Effective Date").

Rains County Texas

Name of Company

9/12/2025

Effective Date

This SOW is subject to the Master Services Agreement executed contemporaneously herewith (the "MSA"). Defined terms not otherwise defined herein shall have the meaning accorded to such terms in the MSA. In the event of a conflict between the terms of this SOW and the MSA, the MSA shall control unless expressly otherwise agreed herein.

1. DEFINITIONS

1.1 "Notification Recipients" means those individuals receiving a notification that they were possibly affected by a breach incident due to exposure of information owned or controlled by Company.

1.2 "Usage-Based" refers to a fee that is charged according to the number or quantity of services provided, including, for example, those based on the number of telephone calls received, number of enrollments, or number of letters mailed.

1.3 "Population-Based" refers to a fee that is calculated and charged up-front based on a specified number of Notification Recipients/individuals to be covered by the services. If the services are thereafter to be extended to additional individuals, an additional Population-Based fee will apply.

2. BREACH SERVICES

Subject to the terms and conditions set forth herein, including payment of the applicable fees, CyberScout shall provide to Company those Breach Services set forth in this SOW. Exhibit A describes the available Breach Services and Exhibit B indicates the specific Breach Services to be provided under this SOW and the applicable fees.

3. TERM

This SOW will commence on the Effective Date and will continue in effect until the conclusion of the Service Period indicated in Exhibit B, unless earlier terminated or extended in accordance with the terms of this Agreement.

4. FEES

4.1 Upfront Fees. Within ten days of the Effective Date, without requiring any invoice or additional action by CyberScout, Company shall pay CyberScout (a) all Set-up Fees set forth in Exhibit B and (b) the Total Population-Based Fee, if any, set forth in Exhibit B, according to the payment instructions set forth in Exhibit C. Company shall also submit the additional required documents specified in Exhibit C, if any, concurrently with making payment. If the fees and additional required documents referred to in this Section 4.1 are not received within ten days after the Effective Date, CyberScout may, in its sole discretion, immediately terminate this SOW by giving written notice to Company.

4.2 Usage-Based Fees. The Usage-Based Fees, if any, set forth in Exhibit B shall be invoiced monthly in arrears based on the services provided and fees incurred in the previous month. Company shall pay the Usage-Based Fees within ten days of the date CyberScout's invoice is forwarded to Company.

5. INVOICING AND PAYMENT

5.1 CyberScout shall forward all invoices to the address of Company set forth in the MSA, and all such invoices are due and payable by Company within ten (10) days of the date each such invoice is forwarded to Company. The fees referred to in Section 4.1 of this SOW are payable in accordance with Section 4.1 and shall not require an invoice. All fees are exclusive of any applicable value-added tax.

5.2 Any payment not received by the due date, at the discretion of CyberScout, may be subject to a late fee of up to 1.5% of the outstanding amount per month.

6. SERVICE HANDLING

Company shall refer each Notification Recipient to CyberScout in the following manner:

For any Call Handling Services, Proactive Fraud Assistance, and ID Fraud and Theft Resolution Services included in this SOW, Notification Recipients will need to call CyberScout at a telephone number to be provided by CyberScout. Notification Recipients must reference their unique identifiers ("Codes") in order for CyberScout to verify their eligibility and provide service. CyberScout shall have no further obligation to verify an individual's identity.

For any Remediation Product Option included in this SOW, Notification Recipients will need to sign up and enter their Code at a secure URL to be provided by CyberScout. The enrollment period is limited to ninety (90) days.

The Codes will be generated and provided to Company by CyberScout. Alternatively, if agreed upon by the parties, Company will generate the Codes and in such case will provide, by secure file transfer, a spreadsheet of the Notification Recipients and associated Codes, which shall not contain any Personal Information.

With the exception of any agreed-upon Notification Services to be provided by CyberScout under this SOW, Company shall distribute the Codes to Notification Recipients in Company's sole discretion and shall be solely responsible for the drafting,

preparation, printing and sending of notification letters/messages to affected Notification Recipients, and all costs associated therewith. Any descriptions of CyberScout's products or services shall use wording provided by CyberScout or approved in advance in writing by CyberScout. If the Breach Services include a Remediation Product Option that includes Expense Reimbursement, Company acknowledges that the notification must include a copy of the Summary Description of Benefits.

7. LANGUAGE SUPPORT

CyberScout's Services are provided primarily in the English language. Additional languages may be available as set forth in a written agreement executed by both Parties.

8. ADDITIONAL TERMS APPLICABLE TO ADDRESS SERVICE

With respect to any "Address Append" services to be provided under this SOW (if applicable), and notwithstanding any contrary provision in the MSA:

Company will submit to CyberScout, via secure means, a file containing the individuals' names and known addresses, or other acceptable data elements that may be agreed upon (e.g., SSN). Company represents that the individuals whose information is disclosed to CyberScout hereunder are United States residents/citizens. Company is responsible for ensuring that the provision of the information to CyberScout does not violate any applicable law or regulation and that Company has obtained any necessary consents from the individuals.

CyberScout will obtain mailing addresses, where available, for the individuals from a third party vendor (the "Address Vendor"), which will require CyberScout to disclose the file to the Address Vendor.

Any mailing addresses or other contact information received from the Address Vendor will not be used by CyberScout or Company for any purpose other than the Notification Services, and both CyberScout and Company will otherwise hold the information in strict confidence. Company will reasonably cooperate with CyberScout and the Address Vendor in the

event the Address Vendor elects to audit the parties' compliance with this requirement. In such event, any audit will occur on new fewer than five (5) business days' notice during normal business hours and will not entail access to any information other than (a) the actual information provided and the way(s) in which it has been used; and (b) the parties' security processes and procedures applicable to the handling of the information. Any information disclosed by Company in connection with such an audit will be maintained as confidential.

Any Address Vendor used in connection with this service is not bound by the terms of the MSA and, specifically, may not comply with the provisions of Sections 4.1 and 6.3 of the MSA. CyberScout agrees to use its best efforts to secure the Address Vendor's contractual agreement to comply with all applicable federal and state laws, rules, and regulations relating to the performance of its services, including any privacy and data protection and security laws. Notwithstanding the provisions of Section 4.1 of the MSA, CyberScout shall not be responsible for the Address Vendor's storage or use of the information disclosed to the Address Vendor in connection with the services set forth in this section; including, but not limited to any failure to safeguard such information.

Company understands and agrees that any information furnished as part of the Address Append or Notification Services is obtained by and through fallible human sources and that for the fees charged, CyberScout and the Address Vendor cannot be an insurer of the accuracy of the information. Company understands and agrees that the correctness, completeness, currentness, merchantability, or fitness for a particular purpose of any information furnished is not guaranteed. Company releases CyberScout and the Address Vendor and their agents and employees from liability, even if caused by negligence, for any loss or injury arising out of or relating to: (a) the accuracy or validity of the information; or (b) any acts or omissions in procuring, reporting or transmitting the information.

(Signature Page Follows after Exhibits)

*"Notwithstanding anything to the contrary herein stated, To the extent permitted by the Constitution and laws of the State of Texas, each party shall be responsible for its own acts and omissions, and the County shall not indemnify or hold harmless any other Party. Nothing in this Agreement shall be construed as a waiver of the County's governmental immunities of defenses under Texas law, including the Texas Tort claims Act."

EXHIBIT A TO STATEMENT OF WORK

Notification Letters (Print and Mail) -- Provides print and mailing services as part of the notification to impacted parties. Includes provision of notification letter template(s) and/or service enrollment document template(s) for use by Company and/or its legal counsel in structuring and developing their breach notification letter(s). Also includes management, handling, printing, and mailing of letters. Final review and evaluation of letter design, formatting, content and compliance with applicable regulations and legal requirements regarding form and content of notification is the sole responsibility of Company.

Notification: Address Append -- Based on information provided by the client, CyberScout obtains addresses for the impacted parties, to be used for purposes of sending the notification to impacted parties.

Notification Letters (Alternate Format) -- As mutually agreed, CyberScout can assist with alternate forms of notification, which may include, for example, sending notice via e-mail or distributing press releases.

Call Handling Services -- Provides scripted responses via FAQs from customer service representatives (CSRs) to impacted parties in compliance with notification laws. Includes:

- Initial call handling to answer questions surrounding notification letter/message or issues with product sign up (in cases where product is offered).
- Issues requiring escalation to the client are determined on a project basis, but typically include non-breach-related questions or questions involving details not available to CSRs. CyberScout is sensitive to clients' capacity to receive such calls and will attempt to resolve issues to a caller's satisfaction before escalating a complaint or question to the client. CyberScout tracks reported issues and communicates them to the client in a weekly summary report.

Proactive Fraud Assistance -- For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access to a fraud specialist who will work with notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Includes:

- Initial credit file activity review with TransUnion (United States only).
- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Identity Theft and Fraud Resolution Services -- Resolution services for Notification Recipients who fall victim to an identity theft as a result of a breach activity. Includes, but is not limited to:

- Unlimited access to a personal fraud specialist via a custom toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes
- All phone calls needed for credit grantor notification, and fraud information removal purposes
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.

- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only).
- Customer service support for individuals when enrolling in optional monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)
- A full year of service, including follow-up calls

* Call Handling, Proactive Fraud Assistance, and ID Theft/Fraud Resolution Services, if provided under this SOW, shall be provided for ninety (90) days (the "Call-Handling Period"). For avoidance of doubt, even if Exhibit B specifies a longer service period for this SOW, the Call-Handling Period shall remain ninety days unless Exhibit B specifically refers to extending the Call-Handling Period.

Remediation Product Options

United States

Single-Bureau Credit Report (1BCR)
 Single-Bureau Credit Monitoring (1BCM)
 Triple-Bureau Credit Report (3BCR)
 Triple-Bureau Credit Monitoring (3BCM)
 Payday Monitoring (Payday)
 Sex Offender Monitoring (Sex Offender)
 Court Records Monitoring (Court Records)
 Public Records Monitoring (Public Records)
 Cyber Internet Surveillance (Dark Web / Cyber)
 Identity Theft Expenses Insurance (\$1,000,000) – see Summary Description of Benefits for details; cannot be provided as a stand-alone product

* All credit/identity monitoring products are delivered electronically over the Internet. Identity Theft Expenses Insurance will be underwritten by certain underwriters at Lloyd's and the entitlements, limitations and restrictions will be as set forth in the insurance policy and its endorsements, which are summarized in the Summary Description of Benefits. The aggregate limit of insurance may be described in currencies other than United States Dollars for communication purposes but such communications will make clear that the total amount that can be claimed will not exceed \$1,000,000 USD.

Consulting Services

Optional forensic consulting services are available under a separate statement of work at an hourly rate.

EXHIBIT B TO STATEMENT OF WORK

The applicable Services and fees for this SOW are indicated in Table 1 (marked with ☒). If a Population-Based Fee is indicated for any Services, refer to Table 2 for details.

The service period is ninety days. However, if the Services include a Remediation Product Option, the service period shall continue until 12 months after the last Product enrollment that occurs during the 90-day enrollment window described in Section 6 of this SOW.

TABLE 1

Check if Included	Service	Fees		
		Set-up Fee	Usage-Based Fee	Population-Based Fee
☒	Notification – Print / Mail Includes up to 2 sheets, front and back, black and white Includes 4 letter versions		Included in flat rate below	
☒	Additional letter versions beyond 4		\$200 per version	
☒	PDF Copies of letters sent (if needed)		\$0.015	
☒	Address Append (if needed)		\$.25 / record	
☒	Data Cleanup (if needed)		\$150 / hour	
☒	90 day call center services - FAQ Support - Toll-Free Number		Included in flat rate	
☒	Adults TransUnion Credit Monitoring, Report and Score Identity Protection Services Identity Resolution Services \$1,000,000 Identity Theft Insurance Minors/Deceased Dark Web Monitoring Identity Protection Services Identity Resolution Services \$1,000,000 Identity Theft Insurance		Flat Rate \$250.00 *The option above includes up to 5% of the population needed two-years of service at no additional charge	

EXHIBIT C TO STATEMENT OF WORK

Electronic Payments to Sontiq, Inc. dba CyberScout	
*** Please send ACH payment remittance to: accountsreceivable@sontiq.com	
For Wire Transfers: To be provided	For ACH delivery: To be provided

Executed and delivered by the parties' authorized representatives on the last date indicated below.

Constangy, Brooks, Smith & Prophete, LLP

Sontiq, Inc. dba CyberScout

Signature of Authorized Representative

Signature of Authorized Representative

Print Name of Signer

Print Name of Signer

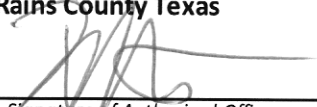
Print Title of Signer

Print Title of Signer

Date Signed

Date Signed

Rains County Texas



Signature of Authorized Officer

Print Name of Signer Brent D. Hilliard

Print Title of Signer County Judge

Date Signed 10-10-2025



COUNTY OF RAINS

BRENT D. HILLIARD

COUNTY JUDGE



RESOLUTION 100925IVB2

STATE OF TEXAS

COUNTY OF RAINS

BE IT REMEMBERED, at a regular meeting of the Commissioners Court of Rains, Texas, held on the 9th day of October, 2025, on motion made by Commissioner of Precinct __ and seconded by Commissioner of Precinct __, the following Resolution was adopted:

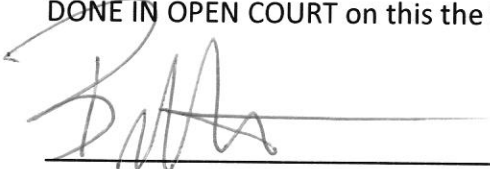
WHEREAS, the County desires to protect its citizens from a breach of security and fraud caused by cyber threats; and

WHEREAS, certain conditions exist which represent a threat;

NOW, THEREFORE, BE IT RESOLVED that the Commissioners Court of Rains, Texas:

Supports the approval of an agreement made with CyberScout to provide services in an effort to minimize this threat and the Commissioners Court directs and designates the County Judge as the County's Chief Executive Officer and Authorized Representative to act in all matters now or hereafter in connection with this agreement.

DONE IN OPEN COURT on this the 9th day of October, 2025.


Brent D. Hilliard, County Judge


JEREMY COOK, COMMISSIONER PRECINCT 1


MIKE WILLIS, COMMISSIONER PRECINCT 2


KOREY YOUNG, COMMISSIONER PRECINCT 3


LORI NORTHCUTT, COMMISSIONER PRECINCT 4

TEL: (903) 473-5000

FAX: (903) 473-4298

BRENT.D.HILLIARD@CO.RAINS.TX.US

167 E. QUITMAN STREET, STE. 102
EMORY, TEXAS 75440