

COMMONWEALTH OF PENNSYLVANIA



BUREAU OF AUDITS

REPORT ON

DEPARTMENT OF TRANSPORTATION

Sterling Infosystems, Inc.
Compliance with Agreement No. 7303208

For the Period
September 17, 2011 to January 6, 2016

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

TABLE OF CONTENTS

	<u>Page</u>
BACKGROUND	1
AUDITOR'S REPORT	2
FINDINGS AND RECOMMENDATIONS	
Finding No. 1: Inadequate Controls Over the Use of Personal Information	6
Finding No. 2: Customer Agreements Lacked Required Provisions	8
Finding No. 3: Inaccurate Customer Listing	12
Finding No. 4: Customers Reselling PennDOT Driver Records.....	15
Finding No. 5: Inadequate Security.....	17

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

BACKGROUND

Acxiom Information Security Systems (Acxiom) signed an Agreement with PennDOT in September 2010 which allowed them to provide their customers PennDOT driver records for employment and insurance purposes. Sterling Infosystems, Inc. (Sterling) purchased Acxiom in January 2012. At that time, all of their operations, personnel and contracts, including their agreement with PennDOT (No. 7303208), were transferred to Sterling.

According to Sterling's website, they are the world's largest company focused entirely on background checks. Their employment screening services include criminal background checks, previous employment verification, educational credential verification, and drug testing. Their website also indicates that Sterling provides full motor vehicle record (MVR) background checks which detail: license type and class, restrictions, expiration date, endorsements, suspensions or revocations, violations/tickets, accidents, and DUIs. Sterling provides these services to many industries including healthcare, education, government, retail, utilities, energy, and transportation.

Sterling requests driver records from PennDOT on behalf of their customers

Sterling provides the driver license number, the driver's last name, and the employer's customer account number when requesting records. PennDOT then provides driver record information such as the driver's name, address, driver number, zip code, date of birth, class of license, record type, license issue and expiration dates, accident information as permitted by law, and all violations and departmental actions for the prior three- or ten-year period.

The agreement between Sterling (originally Acxiom) and PennDOT was set to expire during

The overall objective of this audit is to determine if Sterling complied with the contract provisions of Agreement No. 7303208 and maintained the confidentiality and security of PennDOT's driver record information when providing it to their customers.

Kurt J. Myers
Deputy Secretary for Driver and Vehicle Services
Pennsylvania Department of Transportation
1101 South Front Street
Harrisburg, PA 17104

We have conducted a performance audit to determine if Sterling Infosystems Inc. (Sterling) complied with the terms of Agreement No. 7303208 with the Pennsylvania Department of Transportation. The scope of our audit, except as otherwise noted, was for the period September 17, 2011 through January 6, 2016. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit objective, along with the scope, methodology and conclusion for the audit objective, are as follows:

<i>Audit Objective</i>	Determine if Sterling is in compliance with the terms of Agreement No. 7303208 with the Pennsylvania Department of Transportation (PennDOT).
<i>Methodology/Scope</i>	Documents reviewed in determining Sterling's compliance with Agreement No. 7303208 included customer listings, customer agreements, Affidavits of Intended Use, PennDOT invoices, performance bonds, and reporting on IT controls. Inquiries to both Sterling and PennDOT personnel preceded and followed document reviews.
<i>Conclusions</i>	<u>Sterling Affidavit of Intended Use</u> Although, Sterling filed Affidavits of Intended Use with PennDOT annually using PennDOT's forms as required by the agreement, they were unable to provide the forms for 2011 through 2014. Sterling did provide a copy of their completed Affidavit of Intended Use form for 2015, which was filed with PennDOT on December 30, 2015. <u>Customer List</u> Sterling did not annually provide PennDOT with a list of their customers, see Finding No. 1.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

Audit Objective
Conclusions
(Continued)

In addition, Sterling was unable to provide a complete and accurate listing of their customers or reports identifying the number of records they provided by PennDOT subaccount. The subaccount should identify each client or customer. The number of customers Sterling identified via the two (2) customer lists they provided differed dramatically versus

As it is imperative that PennDOT can rely on Sterling to be able to identify the specific entity that they provide each driver record, their practice of identifying numerous customers or clients with the same subaccount is problematic, see Finding No. 3

Customer Agreements and Affidavits of Intended Use

Sterling was unable to provide three (3) of the thirty-eight (38) requested customer agreements. As indicated in Finding No. 2, the twenty-two (22) customer agreements tested did not contain all of the provisions required by the PennDOT agreement. However, some of those provisions were included in the Affidavits of Intended Use signed by the customers. With the exception of the documents for

only two of the required provisions were not included in either the customer agreement or the Affidavit of Intended Use signed by the customer. The two (2) provisions not included in either the customer agreement or Affidavit of Intended Use were the provisions restricting retaining driver information to employee employment history files and prohibiting creating a file to develop their own source of driver record information. (Sterling was unable to provide an Affidavit of Intended Use for

Sterling has not entered into written customer agreements with all customers who received PennDOT personal information, see Finding No. 4. Some of the entities obtaining information from Sterling actually have agreements with other Sterling customers rather than directly with Sterling. Although it appears that these other customers are resellers, their role is not clear.

Positive Balance for Escrow Account

Between October 2013 and November 2015, there were three instances in which Sterling did not maintain a positive balance in their escrow account.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

Audit Objective
Conclusions
(Continued)

Performance Bond

As evidenced by an Axiom performance bond dated August 2010 and a Sterling performance bond dated October 2013, Axiom/Sterling obtained and maintained in full force and effect a performance bond for the benefit of PennDOT.

Subcontractors

Sterling retained the services of and as data centers during the audit period. Sterling did not seek PennDOT approval of these subcontractor arrangements, and they did not require either company to complete Affidavits of Intended Use.

Data Security

Sterling was unable to provide assurance that they and their customers and data centers have implemented controls adequate to ensure that personal driver record information is safeguarded.

As outlined in Finding No. 5, Sterling provided an ISO 27001 certificate rather than a Service Organization Control (SOC) report. The American Institute of Certified Public Accountants (AICPA) issued Statement on Standards for Attestation Engagements (SSAE) No. 16 along with the framework of three (3) SOC reports that involve reporting on controls at a service organization. Each of the three SOC reports involves different levels of testing. Unlike a SOC report, the ISO certificate Sterling provided does not cover the design and effectiveness of controls related to the following principles: security, availability, confidentiality, processing integrity, and privacy.

Sterling provided SOC reports for their two data centers, and. While Sterling asserted that they requested a report from it appears that the report provided is actually a report. A SOC 1 report is designed to report on controls over financial reporting. The report disclosed an exception in regards to separated employees. uses key card access to limit access to their data center facilities, and testing for key card access to facilities determined that seven (7) terminated employees sampled had access to facilities.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016


<i>Audit Objective</i>	During the exit conference, Sterling indicated that they would
<i>Conclusions</i>	prefer to have a _____ report from each
<i>(Continued)</i>	subcontractor rather than a _____ report, and they are
	planning on having a Sterling _____ report available
	by 2017 due to the _____
	for such a report.
<i>Related Findings and</i>	
<i>Recommendations</i>	See Finding No. 1 through Finding No. 5

Internal Controls

In planning and performing our audit, we considered internal controls that are significant within the context of our audit objective and assessed whether such controls had been properly designed and implemented. Based on our assessment of the internal controls, we determined audit procedures for the purpose of reporting on our audit objective, but not to provide assurance on Sterling's internal control. Any significant control deficiencies that came to our attention during the audit are included in the findings section of this report.

The Sterling response to our findings is described in the findings sections of this report. We did not audit the Sterling response.

This report is intended solely for the information and use of Sterling, PennDOT and Office of Budget management and is not intended to be and should not be used by anyone other than these specified parties.



Jenny Richter, CPA
Assistant Director Regional Audits

January 6, 2016

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 1 – Inadequate Controls Over the Use of Personal Information

Sterling was unable to provide evidence that they filed Affidavits of Intended Use between 2011 and 2014. They filed an Affidavit of Intended Use for 2015 on December 30, 2015. Sterling was also not able to provide one (1) of the thirty-eight (38) requested customer Affidavits of Intended Use. In addition, Sterling does not annually provide a list of their customers to PennDOT.

Section 3(a), Reporting Requirements, in Agreement No. 7303208 between PennDOT and Sterling states: "The Contractor agrees to file annually with the Department an "Affidavit of Intended Use" on the form prescribed by the Department, to be kept on file by the Department.

Section 3(c), Maintenance of Records, in Agreement No. 7303208 between PennDOT and Sterling states: "The Contractor agrees to have each of its customers and subcontractors complete and "Affidavit of Intended Use" on a form prescribed by the Department. The Contractor agrees to keep the "Affidavits of Intended Use" for its customers and subcontractors on file at a central location during such party's access to Pennsylvania driver record information under this Agreement and for three years thereafter. The Contractor will provide the Department annually a complete list of all customers and subcontractors for which they have an "Affidavit of Intended Use" on file. The Contractor shall also require their subcontractor to keep on file the "Affidavits of Intended Use" or such other document acceptable to the Department for their employees at a central location during the employee's access to Pennsylvania driver record information under this Agreement and for three years thereafter. Upon the request of the Department, the Contractor will provide copies of the "Affidavits of Intended Use" to the Department."

Sterling asserted that the reason they didn't have the one (1) requested affidavit was that an employee did not maintain copies of all affidavits, further stating the employee has since been terminated. It is unclear why Sterling did not file an Affidavit of Intended Use with PennDOT themselves or annually provide a list of their customers to PennDOT.

Without copies of the signed Affidavits of Intended Use, Sterling cannot affirm that Sterling or their customers are aware of the restrictions listed on the affidavits. Because Sterling did not provide a list of customers, there is a risk that Sterling provides records to customers that PennDOT has approved.

Recommendations

We recommend that Sterling annually file an Affidavit of Intended Use with PennDOT and keep a copy on file. Sterling should also maintain copies of all Affidavits of Intended Use for its customers and subcontractors and provide annually, a list of all customers and subcontractors for which they have an Affidavit of Intended Use on file.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 1 – Inadequate Controls Over the Use of Personal Information (Continued)

Audited Entity Response

Sterling has provided a signed Affidavit to PennDOT for 2015 and will continue to do so annually as required. Sterling will also provide a list of customers to PennDOT annually. A full company listing is attached here as well.

Auditor Conclusion

The finding and recommendation remain as stated.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 2 – Customer Agreements Lacked Required Provisions

Seventeen (17) active customer agreements executed between July 2001 and February 2011 by predecessor companies and Acxiom Information Security Services) and five (5) Sterling customer agreements executed between 2014 and 2015 were reviewed to determine if they contained the provisions required by the agreement with PennDOT. As illustrated in the Agreement Provision Compliance Schedule at the end of this finding, the customer agreements did not contain all of the provisions required by the PennDOT agreement. Some of the missing provisions were included in the customer Affidavits of Intended Use. However, two of the required provisions were not included in either the customer agreement or the Affidavit of Intended Use signed by the customers. Those two (2) provisions were the provision restricting retaining driver information to employee employment history files and the provision prohibiting creating a file to develop their own source of driver record information. In addition, the agreement did not contain six (6) of the eight (8) provisions tested. Sterling was unable to provide the Affidavit of Intended Use for

The terms and conditions of Paragraph 3 include:

Section 3(i), Required Security, in Agreement No. 7303208 between PennDOT and Sterling, "The Contractor, its customers, and subcontractors shall at all times maintain safeguards and procedures to ensure the security and protection of information furnished by the Department and shall take all necessary steps to prevent the divulgence or use of such information in any form or manner not expressly permitted by this Agreement. This security shall include written agreements between Contractor and its customers..." The terms and conditions of Section 3 of the Agreement include:

Section 3(d), Use of Information, "The Contractor agrees that it shall enter into written agreements with any and all customers, and that those agreements shall include a provision that expressly states that the customer shall not sell, assign, or otherwise transfer any information or portions or information obtained pursuant to this Agreement to any third party. Customer agreements shall also expressly limit the use of any obtained driver record, in whole or in part, to insurance or employment purposes."

Section 3(e), Restriction Against Publication, "Except as provided for in Paragraph (d), under no circumstances shall the Contractor use or permit others to use any information provided by the Department for direct or electronic mail advertising or any other type or types of mail or mailings. The Contractor shall not disclose or publish the names, addresses, or other personal information appearing in any driver record to any individual or group other than the Contractor's approved customer and Contractor shall exercise a high degree of care to hold and maintain all record information not within the parameters of information to be released in the strictest confidence and carefully restrict access to this information."

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 2 – Customer Agreements Lacked Required Provisions (Continued)

Section 3(f), Contractor Databases, “The Contractor and its customers will be the sole users of driver record information supplied by the Department. Driver record information supplied by the Department shall not be used to create or update a file to be used by the Contractor, its customers, or subcontractors to develop their own source of driver record information. Driver record information shall not be retained, stored, combined, and/or linked in with any other data on any database by the Contractor, its customers, or subcontractors for any reason. The contractor and their customers who obtain driver information for insurance purposes are permitted to retain driver record information only for as long as is necessary to conduct insurance business or as may be required by law. Employers may retain the information only in the employee’s employment history file. Subcontractors are not permitted to retain any driver record information.

Section 3(g), Internet Prohibition, “The Contractor agrees not to disseminate or publish on the internet the personal information obtained from the Department or to allow any other person to disseminate or publish the personal information on the internet without the written approval of the Department.”

Section 3(h), Ownership of Records, “The Department retains exclusive proprietary ownership of all driver record information provided under this Agreement.”

It is not clear why some of the customer agreements did not 1) restrict the customer from using the driver record information supplied by PennDOT to create or update a file to be used to develop their own source of driver record information or 2) state that the customer should only retain the information in the employee’s employment history file.

As Sterling was unable to provide an Affidavit of Intended Use for any provisions that may have been included in the document are unknown.

Absence of required customer agreement language, replicating Section 3 provisions of Agreement No. 7303208 between Sterling and PennDOT, increases the potential that personal information obtained from PennDOT will be divulged or used in a manner not expressly permitted by the Agreement.

Recommendations

We recommend that PennDOT ensure Sterling obtains assurance that their customers understand and agree to comply with the restrictions detailed in any wholesale data agreement with PennDOT, currently Agreement No. 7303208.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 2 – Customer Agreements Lacked Required Provisions (Continued)

We further recommend that Sterling update their customer agreements to include all provisions required by their Agreement with PennDOT.

Audited Entity Response

Regarding the provision restricting retaining driver information to employee employment files, prior to the procurement of background screening reports, SterlingBackcheck credentials clients (End User Certification/Credentialing Application). As part of the process, clients must certify the purpose for which they are procuring the reports. We do not deliver PennDOT information to any clients unless it's for employment purposes. Accordingly, by default, SterlingBackcheck's clients are placing the information from PennDOT with the other background screening report information, i.e. into employee employment history files.

Regarding the provision prohibiting creating a file to develop their own source of driver record information, Section 3.1 of the Master Service Agreement restricts clients from providing "any part of the Services to others, whether directly or indirectly, through incorporation in a database, report or otherwise."

In regards to the AISS agreements, the first agreement is deficient in both respects as per what PennDOT is requesting. The 2nd and 3rd agreements we believe cover what PennDOT is looking for. In both, Section A(3) limits client's requests to being made for employment purposes. Again, this limits the driving record information to be stored in employee's employment files. Additionally, Section 5 in both limits disclosure only to the "current employment decision" and states that the clients cannot share with any other third parties. Accordingly, they are restricted from developing their own source of driver record information.

Auditor Conclusion

The finding and recommendation remain as stated.

Finding No. 2 – Agreement Provision Compliance Schedule

7	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526
---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 3 – Inaccurate Customer Listing

Sterling was unable to provide a complete and accurate listing of their customers. They initially indicated they had approved customers. The customer listing provided with this assertion contained more than one subaccount for the same customer. When these duplicates were accounted for, the list contained unique customer names.

The listing that Sterling provided in October of 2015 contained the names of clients associated with PennDOT approved subaccount numbers. of these clients were associated with just subaccounts. The number of clients associated with each of these subaccounts varies from clients. While some of companies are closely related, for instance, others appear to be diverse companies that would not have the same FIN, like the clients associated with subaccount A few of the client names in this subaccount are

It appears that both of the Sterling provided customer listings were incomplete because Sterling utilizes and neither of the provided lists identified In addition, the listing of approved Sterling customers provided by PennDOT did not contain customers identified by Sterling as being PennDOT approved.

It is unclear if Sterling maintains a record of the end user for each request for driver information submitted to PennDOT. They assert that their system can report on the daily number of records requested by each customer (non-method specific); however, the report does not include the customer subaccount number or indicate the method used to obtain the records from PennDOT Sterling indicated that they utilize the to ask for records for customers that PennDOT has

Section 3(c), Maintenance of Records, in Agreement No. 7303208 between PennDOT and Sterling states: "The Contractor will provide the Department annually a complete list of all customers and subcontractors..."

Section 3(j), End User Requestor Information, in Agreement No. 7303208 between PennDOT and Sterling states: "The Contractor is required to submit end user information electronically to the Department with each driver record request. The Contractor is required to maintain a record of the end user for each request for driver information submitted to the Department. Upon the request of the Department, the Contractor will provide the name, address, and telephone number of the end user."

It is unclear why Sterling was unable to provide a complete and accurate listing of their customers.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 3 – Inaccurate Customer Listing (Continued)

The reason the first Sterling-provided listing contained duplicate names is also not clear, as PennDOT indicated the one group of [redacted] associated with the duplicate names originated with Axiom when they were obtaining records as a pre-employment business customer (identified by subaccount numbers containing [redacted] and Sterling had requested new [redacted] to obtain records for the same customers as a wholesale data provider. The [redacted] for these customers contained [redacted] which PennDOT stated identifies them as Sterling wholesale data provider requests [redacted] rather than a pre-employment business customer request [redacted]. Conversely, Sterling asserted the duplicate names with [redacted] in the [redacted] were associated with [redacted] a company they utilized for background screenings. It does appear that Sterling is maintaining the [redacted] with these [redacted] which identify them as the recorded requestor, to request records as a background screening company, using the on-line process to obtain the records and to request records (for the same customers) as a [redacted] using the [redacted].

According to PennDOT, the reason the list they provided did not contain the [redacted] customers identified by Sterling as approved was because PennDOT did not include the customers approved for Sterling as a background screening company, explaining that customers are approved for them to provide information as a wholesale data provider and as a background screening company. As indicated previously, the difference between the two listings is that the [redacted] associated with each identify how the driving record will be [redacted].

Sterling did not indicate why their system is unable to report on the number of records requested on behalf of each entity.

As many of the companies making up the [redacted] clients Sterling assigned to just [redacted] PennDOT appear to be separate entities that would have separate Federal Identification Numbers (FIDN), it is doubtful that they are properly identified and approved by PennDOT. In addition, when the actual customer is not identified as in the situation where numerous clients are identified to the same subaccount number, there is an increased risk that these parties have not signed customer agreements or Affidavits of Intended Use, thereby making it more likely that they will not comply with restrictions that should be identified in these documents.

If Sterling is unable to provide a complete and accurate listing of their customers, the risk is increased that they also cannot identify the specific data that has been provided to each customer. Further, utilizing a system which cannot accurately and efficiently produce reports identifying the records provided to each entity increases the risk that the responsible party would not be identified if there was a security breach.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 3 – Inaccurate Customer Listing (Continued)

Recommendation

We recommend that PennDOT require Sterling to provide a current complete and accurate listing of their customers. The listing should indicate if Sterling has more than one identification number for any customer and whether the customer has a unique Federal Identification Number (FIN). The listing should also indicate if more than one client is associated with a customer number and if all clients associated with the customer number operate under the same FIN.

Audited Entity Response

Axiom was acquired by Sterling Infosystems in December 2011. Customers continue to place orders on this platform (AISS/Axiom) until these clients

is used for new customers onboarded directly with Sterling
is related to
When the audit began, the focus was on
and Axiom customers
processed via
Axiom requests are

The AISS platform use

for example are all

We can provide every PA MVR requested for each individual and the end user if requested. Our reports do not indicate the ordering/processing method for that request

We would have to cross reference different reports to accomplish that. However, the end user can be identified and only processed electronically i

Auditor Conclusion

The finding and recommendation remain as stated.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 4 – Customers Reselling PennDOT Driver Records

A number of Sterling customers are actually resellers. Although the resellers appear to be providing the information to entities identified with an approved subaccount, PennDOT is not aware the information is passing through this 3rd party. In addition, Sterling does not enter into customer agreements with the customers provided driver records through these resellers; rather the reseller has an agreement with the customers.

One reseller was identified because Sterling was unable to provide requested customer agreements. The agreements Sterling could not

provide were for Sterling explained that these two customers were Both had agreements with but only had an agreement with Sterling. The agreement between and Sterling indicates that any entity may purchase services and may also purchase services on behalf of laboratories for which it provides management services. Sterling was not able to provide the agreements which entered into with Both filed Affidavits of Intended Use with PennDOT and were provided their own customer subaccount number. Requests which made through Sterling on behalf of were submitted to PennDOT under customer subaccount numbers rather than subaccount number. It is important to note that the subaccount represent entities. It is unknown if they all operate under the same PIN. According to PennDOT, Sterling did not request PennDOT's approval to have customers provide PennDOT driver records to third parties.

In addition to Sterling being unable to provide two (2) of customer agreements requested, a review of the customer agreement for revealed that the customer agreement was actually a contract between and It is unclear if obtains driver records as a subcontractor of Sterling and then provides them to an additional subcontractor or directly to their customers.

Section 3(d), Use of Information, in Agreement No. 7303208 between PennDOT and Sterling states: "The Contractor agrees that it shall enter into written agreements with any and all customers, and that those agreements shall include a provision that expressly states that the customer shall not sell, assign, or otherwise transfer any information or portions of information obtained pursuant to this Agreement to a third party."

Sterling responded to additional questions related to acting as a reseller of PennDOT driver records by stating that does not resell PennDOT driver records. Sterling also stated that other users that request records separately but are considered as being part of the "Group" for tracking purposes. They have also not identified the number and names of other customers that operate as resellers.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 4 – Customers Reselling PennDOT Driver Records (Continued)

Sterling did respond to requests for clarification regarding the relationship with [redacted] stating that [redacted] was a third party motor vehicle records vendor.

Reseller or subcontractor relationships that are not disclosed and approved by PennDOT increase the risk that PennDOT information will not be used and secured as required and that breaches involving such use will be difficult to prevent and detect.

Recommendations

We recommend that PennDOT require Sterling to obtain direct agreements with all parties they provide PennDOT data and maintain copies of all agreements, including Primary Integration LLC.

We further recommend that PennDOT require Sterling to clarify the relationship between Sterling and Sterling's other customers [redacted] and identify any similar arrangements with companies other than [redacted] so PennDOT can determine if these arrangements comply with Sterling's agreement with PennDOT.

Audited Entity Response

Sterling does not resell PennDOT driver records. PennDOT driver records were not provided to [redacted] then to the end user. End Users have individual accounts in our system with signed Affidavits of Intended Use. Reports are provided directly to the end user. These clients may be referenced as being part of the [redacted] "Group" for tracking purposes.

[redacted] was a 3rd party MVR vendor who provided reports mainly in [redacted] no longer a vendor.

Auditor Conclusion

The finding and recommendation remain as stated.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 5 – Inadequate Security

Sterling provided an ISO 27001 certificate in response to a request for a Service Organization Control (SOC) report. Unlike a SOC 2 report, an ISO 27001 certificate does not report on the design and effectiveness of controls related to the following principles: security, availability, confidentiality, processing integrity, and privacy.

Sterling was able to provide SOC reports for their two data centers, which are

The SOC report provided for the primary data center, was identified as a SOC 1, Type 2 report, which as disclosed in the report is intended to provide information to the auditor of a user entity's financial statements about controls at a service organization.

The SOC report provided for the secondary data center, did not identify the type of report. However, the content indicates it is a SOC 2, Type 2 report, the subject of which would be beneficial in assessing whether the entities controls are adequate over security, availability, processing integrity confidentiality, and privacy. The provided report identified some exceptions related to the monitoring of security access to buildings. In addition, they did not test some controls such as controls over the movement of restricted data and controls to prevent and detect unauthorized or malicious software.

As an organization that provides personal motor vehicle information to customers, there is a need for assurance that the information remains secure whether it is with Sterling or some other entity that they have provided the information.

Section 3(i), Required Security, in Agreement No. 7303208 between PennDOT and Sterling states: "The Contractor, its customers, and subcontractors shall at all times maintain safeguards and procedures to ensure the security and protection of information furnished by the Department and shall take all necessary steps to prevent the divulgence or use of such information in any form or manner not expressly permitted by this Agreement. This security shall include written agreements between Contractor and its customers and subcontractors expressly incorporating the terms and conditions of Section 2 of this Agreement and the keeping of driver record information in a controlled access area."

Multiple requests did not result in Sterling providing. It is unclear why Sterling did not obtain an adequate assessment of their controls.

Sterling Infosystems, Inc.
Wholesale Data Provider
Program Agreement No. 7303208
For the Period September 17, 2011 to January 6, 2016

FINDINGS AND RECOMMENDATIONS

Finding No. 5 – Inadequate Security (Continued)

Without an adequate assessment of the relevant controls there is an increased risk that the controls necessary to ensure security, availability, processing integrity, confidentiality, and privacy may not exist or may not be operating properly.

Recommendation

We recommend that PennDOT require that any reports on the internal control environment of Sterling, its customers, subcontractors and data centers provide adequate assurance that PennDOT-provided information is secure and is used in compliance with the confidentiality and privacy requirements of their agreement with PennDOT.

Audited Entity Response

We can, and have, provided SOC 2 reports for our data centers. These reports are in fact both SSAE 16 SOC 2 reports. I do not know where the statement is made that the report is a SOC 1, Type 2 report; it is in indeed a SOC 2 Type 2 report. The report is also SOC 2 Type 2 report.

We have been informed by the data center provider that the exceptions noted with respect to security monitoring have been corrected.

With respect to the gap in testing of "controls over the movement of restricted data and controls to prevent and detect unauthorized or malicious software", we maintain our own infrastructure within these data centers, and those controls are within our ISO 27001 scope, and not within the data center's SSAE 16 SOC 2 scope, since they do not manage or have access to our data or systems.

Auditor Conclusion

The finding and recommendation remain as stated.