

COUNCIL OF THE CITY OF ABERDEEN
Ordinance No. 10-O-16

Introduced By:	Mayor Michael E. Bennett
Date Introduced:	November 15, 2010
Date Adopted:	November 29, 2010
Date Effective:	December 19, 2010

ORDINANCE NO. 10-O-16

AN ORDINANCE TO PROVIDE FOR AN IDENTITY THEFT PREVENTION PROGRAM; TO COMPLY WITH FEDERAL REGULATIONS RELATING TO ADDRESS DISCREPANCIES; AND TO COMPLY WITH FEDERAL REGULATIONS RELATING TO RED FLAGS AND IDENTITY THEFT.

- 1 WHEREAS, pursuant to federal law the Federal Trade Commission adopted Identity
2 Theft Rules requiring the creation of certain policies relating to the use of consumer
3 reports, address discrepancy and the detection, prevention and mitigation of identity theft;
- 4 WHEREAS, the Federal Trade Commission regulations, adopted as 16 CFR § 681.2
5 require creditors, as defined by 15 U.S.C. § 1681a(r)(5) to adopt red flag policies to
6 prevent and mitigate identity theft with respect to covered accounts;
- 7 WHEREAS, 15 U.S.C. § 1681a(r)(5) cites 15 U.S.C. § 1691a, which defines a creditor as
8 a person that extends, renews or continues credit, and defines 'credit' in part as the right
9 to purchase property or services and defer payment therefore;
- 10 WHEREAS, the Federal Trade Commission regulations include utility companies in the
11 definition of creditor;
- 12 WHEREAS, the City of Aberdeen is a creditor with respect to 16 CFR § 681.2 by virtue
13 of providing utility services or by otherwise accepting payment for municipal services in
14 arrears;
- 15 WHEREAS, the Federal Trade Commission regulations define 'covered account' in part
16 as an account that a creditor provides for personal, family or household purposes that is
17 designed to allow multiple payments or transactions and specifies that a utility account is
18 a covered account;
- 19 WHEREAS, the Federal Trade Commission regulations require each creditor to adopt an
20 Identity Theft Prevention Program which will use red flags to detect, prevent and mitigate

21 identity theft related to information used in covered accounts;

22 WHEREAS, the City provides water and sewer services for which payment is made after
23 the service has otherwise been provided which by virtue of being utility accounts are
24 covered accounts;

25 WHEREAS, the Federal Trade Commission regulations, adopted as 16 CFR 681.1,
26 require users of consumer credit reports to develop policies and procedures relating to
27 address discrepancies between information provided by a consumer and information
28 provided by a consumer credit company;

29 WHEREAS, the duly elected governing authority of the City of Aberdeen is the Mayor
30 and Council thereof;

31 NOW THEREFORE BE IT ORDAINED, that the City of Aberdeen adopts the following
32 Identity Theft Prevention Program:

33 **Section 1**

34 The Code of the City of Aberdeen is hereby amended by adding a chapter to be numbered
35 68, Identity Theft: Address Discrepancies, which said chapter reads as follows:

36 “Article I

37 Identity Theft Prevention Program

38 Section 68-1. Short Title.

39 This article shall be known as the Identity Theft Prevention Program.

40 Section 68-2. Purpose.

41 The purpose of this Article is to comply with 16 CFR § 681.2 in order to detect, prevent
42 and mitigate identity theft by identifying and detecting identity theft red flags and by
43 responding to such red flags in a manner that will prevent identity theft.

44 Section 68-3. Definitions.

45 For purposes of this Article, the following definitions apply (*see Note 1*):

46 ‘City’ means the City of Aberdeen.

47 ‘Covered account’ means (i) An account that a financial institution or creditor offers or
48 maintains, primarily for personal, family, or household purposes, that involves or is
49 designed to permit multiple payments or transactions, such as a credit card account,

50 mortgage loan, automobile loan, margin account, cell phone account, utility account,
51 checking account, or savings account; and (ii) Any other account that the financial
52 institution or creditor offers or maintains for which there is a reasonably foreseeable risk
53 to customers or to the safety and soundness of the financial institution or creditor from
54 identity theft, including financial, operational, compliance, reputation, or litigation risks.

55 'Credit' means the right granted by a creditor to a debtor to defer payment of debt or to
56 incur debts and defer its payment or to purchase property or services and defer payment
57 therefore.

58 *Note 1: Other than "City" and "personal identifying information", definitions provided*
59 *in this section are based on the definitions provided in 16 CFR § 681.2.*

60 'Creditor' means any person who regularly extends, renews, or continues credit; any
61 person who regularly arranges for the extension, renewal, or continuation of credit; or
62 any assignee of an original creditor who participates in the decision to extend, renew, or
63 continue credit and includes utility companies and telecommunications companies.

64 'Customer' means a person that has a covered account with a creditor.

65 'Identity theft' means a fraud committed or attempted using identifying information of
66 another person without authority.

67 'Person' means a natural person, a corporation, government or governmental subdivision
68 or agency, trust, estate, partnership, cooperative, or association.

69 'Personal Identifying Information' means a person's credit card account information,
70 debit card information, bank account information, and drivers' license information and
71 for a natural person includes their social security number, mother's birth name, and date
72 of birth.

73 'Red flag' means a pattern, practice, or specific activity that indicates the possible
74 existence of identity theft.

75 'Service provider' means a person that provides a service directly to the City.

76 Section 68-4. Findings.

77 A. The City is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance
78 of covered accounts for which payment is made in arrears.

79 B. Covered accounts offered to customers for the provision of City services include
80 utility accounts.

81 C. The City's previous experience with identity theft related to covered accounts is as

82 follows:

83 The City has no record of identity theft related to water and sewer accounts.

84 D. The processes of opening a new covered account, restoring an existing covered
85 account, and making payments on such accounts have been identified as potential
86 processes in which identity theft could occur.

87 E. The City limits access to personal identifying information to those employees
88 responsible for or otherwise involved in opening or restoring covered accounts or
89 accepting payment for use of covered accounts. Information provided to such employees
90 is entered directly into the City's computer system and is not otherwise recorded.

91 F. The City determines that there is a low risk of identity theft occurring in the following
92 ways (*if any*):

93 (1) Use by an applicant of another person's personal identifying information to establish
94 a new covered account;

95
96 (2) Use of a previous customer's personal identifying information by another person in an
97 effort to have service restored in the previous customer's name;

98 (3) Use of another person's credit card, bank account, or other method of payment by a
99 customer to pay such customer's covered account or accounts;

100 (4) Use by a customer desiring to restore such customer's covered account of another
101 person's credit card, bank account, or other method of payment.

102 Section 68-5. Process of Establishing a Covered Account.

103 A. As a precondition to opening a covered account in the City, each applicant shall
104 provide the City with personal identifying information of the customer [name, address,
105 driver's license or other valid government issued identification card containing a
106 photograph of the customer or, for customers who are not natural persons, a photograph
107 of the customer's agent opening the account.] Such information shall be entered directly
108 into the City's computer system and shall not otherwise be recorded.

109 B. Each account shall be assigned an account number and personal identification number
110 (PIN) which shall be unique to that account. The City may utilize computer software to
111 randomly generate assigned PINs and to encrypt account numbers and PINs.

112 Section 68-6. Access to Covered Account Information.

113 A. Access to customer accounts shall be password protected and shall be limited to
114 authorized City personnel.

115 B. Such password(s) shall be changed by the Information Technology Coordinator on a
116 regular basis, shall be at least 8 characters in length and shall contain letters, numbers and
117 symbols.

118 C. Any unauthorized access to or other breach of customer accounts is to be reported
119 immediately to the Director of Finance and the password changed immediately.

120 D. Personal identifying information included in customer accounts is considered
121 confidential and any request or demand for such information shall be immediately
122 forwarded to the City Manager and the City Attorney.

123 Section 68-7. Credit Card Payments.

124 A. In the event that credit card payments that are made over the Internet are processed
125 through a third party service provider, such third party service provider shall certify that
126 it has an adequate identity theft prevention program in place that is applicable to such
127 payments.

128 B. All credit card payments made over the telephone or the City's website shall be
129 entered directly into the customer's account information in the computer data base.

130 C. Account statements and receipts for covered accounts shall include only the last four
131 digits of the credit or debit card or the bank account used for payment of the covered
132 account.

133 Section 68-8. Sources and Types of Red Flags.

134 All employees responsible for or involved in the process of opening a covered account,
135 restoring a covered account or accepting payment for a covered account shall check for
136 red flags as indicators of possible identity theft and such red flags may include:

137 A. Alerts from consumer reporting agencies, fraud detection agencies or service
138 providers. Examples of alerts include but are not limited to:

139 (1) A fraud or active duty alert that is included with a consumer report;

140 (2) A notice of credit freeze in response to a request for a consumer report;

141 (3) A notice of address discrepancy provided by a consumer reporting agency;

142 (4) Indications of a pattern of activity in a consumer report that is inconsistent
143 with the history and usual pattern of activity of an applicant or customer, such
144 as:

- 145 (a) A recent and significant increase in the volume of inquiries;
- 146 (b) An unusual number of recently established credit relationships;
- 147 (c) A material change in the use of credit, especially with respect to
- 148 recently established credit relationships; or
- 149 (d) An account that was closed for cause or identified for abuse of
- 150 account privileges by a financial institution or creditor.

151 B. Suspicious documents. Examples of suspicious documents include:

- 152 (1) Documents provided for identification that appear to be altered or forged;
- 153
- 154 (2) Identification on which the photograph or physical description is inconsistent
- 155 with the appearance of the applicant or customer;
- 156 (3) Identification on which the information is inconsistent with information
- 157 provided by the applicant or customer;
- 158 (4) Identification on which the information is inconsistent with readily accessible
- 159 information that is on file with the financial institution or creditor, such as a
- 160 signature card or a recent check; or
- 161 (5) An application that appears to have been altered or forged, or appears to have
- 162 been destroyed and reassembled.

163 C. Suspicious personal identification, such as suspicious address change. Examples of

164 suspicious identifying information include:

- 165 (1) Personal identifying information that is inconsistent with external information
- 166 sources used by the financial institution or creditor. For example:
 - 167 (a) The address does not match any address in the consumer report; or
 - 168 (b) The Social Security Number (SSN) has not been issued, or is listed on
 - 169 the Social Security Administration's Death Master File.
- 170 (2) Personal identifying information provided by the customer is not consistent
- 171 with other personal identifying information provided by the customer, such as
- 172 a lack of correlation between the SSN range and date of birth.
- 173 (3) Personal identifying information or a phone number or address, is associated
- 174 with known fraudulent applications or activities as indicated by internal or
- 175 third-party sources used by the financial institution or creditor.
- 176 (4) Other information provided, such as fictitious mailing address, mail drop
- 177 addresses, jail addresses, invalid phone numbers, pager numbers or answering
- 178 services, is associated with fraudulent activity.

- 179 (5) The SSN provided is the same as that submitted by other applicants or
180 customers.
- 181 (6) The address or telephone number provided is the same as or similar to the
182 account number or telephone number submitted by an unusually large number
183 of applicants or customers.
- 184 (7) The applicant or customer fails to provide all required personal identifying
185 information on an application or in response to notification that the
186 application is incomplete.
- 187 (8) Personal identifying information is not consistent with personal identifying
188 information that is on file with the financial institution or creditor.
- 189 (9) The applicant or customer cannot provide authenticating information beyond
190 that which generally would be available from a wallet or consumer report.
- 191 D. Unusual use of or suspicious activity relating to a covered account. Examples of
192 suspicious activity include:
- 193 (1) Shortly following the notice of a change of address for an account, City
194 receives a request for the addition of authorized users on the account.
- 195 (2) A new revolving credit account is used in a manner commonly associated with
196 known patterns of fraud patterns. For example:
197
- 198 (a) The customer fails to make the first payment or makes an initial
199 payment but no subsequent payments.
- 200 (3) An account is used in a manner that is not consistent with established patterns
201 of activity on the account. There is, for example:
- 202 (a) Nonpayment when there is no history of late or missed payments;
203 (b) A material change in purchasing or spending patterns.
- 204 (4) An account that has been inactive for a long period of time is used.
- 205 (5) Mail sent to the customer is returned repeatedly as undeliverable although
206 transactions continue to be conducted in connection with the customer's
207 account.
- 208 (6) The City is notified that the customer is not receiving paper account
209 statements.

210 (7) The City is notified of unauthorized charges or transactions in connection with
211 a customer's account.

212 (8) The City is notified by a customer, law enforcement or another person that it
213 has opened a fraudulent account for a person engaged in identity theft.

214 E. Notice from customers, law enforcement, victims or other reliable sources regarding
215 possible identity theft or phishing relating to covered accounts.

216 Section 68-9. Prevention and Mitigation of Identity Theft.

217 A. In the event that any City employee responsible for or involved in restoring an existing
218 covered account or accepting payment for a covered account becomes aware of red flags
219 indicating possible identity theft with respect to existing covered accounts, such
220 employee shall use his or her discretion to determine whether such red flag or
221 combination of red flags suggests a threat of identity theft. If, in his or her discretion,
222 such employee determines that identity theft or attempted identity theft is likely or
223 probable, such employee shall immediately report such red flags to the Director of
224 Finance. If, in his or her discretion, such employee deems that identity theft is unlikely or
225 that reliable information is available to reconcile red flags, the employee shall convey this
226 information to the Director of Finance, who may in his or her discretion determine that no
227 further action is necessary. If the Director of Finance in his or her discretion determines
228 that further action is necessary, a City employee shall perform one or more of the
229 following responses, as determined to be appropriate by the Director of Finance:

230 (1) Contact the customer;

231 (2) Make the following changes to the account if, after contacting the customer, it
232 is apparent that someone other than the customer has accessed the customer's
233 covered account:

234 (a) change any account numbers, passwords, security codes, or other
235 security devices that permit access to an account; or

236 (b) close the account;

237 (3) Cease attempts to collect additional charges from the customer and decline to
238 sell the customer's account to a debt collector in the event that the customer's
239 account has been accessed without authorization and such access has caused
240 additional charges to accrue;

241 (4) Notify a debt collector within two (2) business days of the discovery of likely
242 or probable identity theft relating to a customer account that has been sold to
243 such debt collector in the event that a customer's account has been sold to a
244 debt collector prior to the discovery of the likelihood or probability of identity
245 theft relating to such account;

246 (5) Notify law enforcement, in the event that someone other than the customer has
247 accessed the customer's account causing additional charges to accrue or
248 accessing personal identifying information; or

249 (6) Take other appropriate action to prevent or mitigate identity theft.

250 B. In the event that any City employee responsible for or involved in opening a new
251 covered account becomes aware of red flags indicating possible identity theft with respect
252 an application for a new account, such employee shall use his or her discretion to
253 determine whether such red flag or combination of red flags suggests a threat of identity
254 theft. If, in his or her discretion, such employee determines that identity theft or
255 attempted identity theft is likely or probable, such employee shall immediately report
256 such red flags to the Director of Finance. If, in his or her discretion, such employee
257 deems that identity theft is unlikely or that reliable information is available to reconcile
258 red flags, the employee shall convey this information to the Director of Finance, who
259 may in his or her discretion determine that no further action is necessary. If the Director
260 of Finance in his or her discretion determines that further action is necessary, a City
261 employee shall perform one or more of the following responses, as determined to be
262 appropriate by the Director of Finance:

- 263 (1) Request additional identifying information from the applicant;
264 (2) Deny the application for the new account;
265 (3) Notify law enforcement of possible identity theft; or
266 (4) Take other appropriate action to prevent or mitigate identity theft.

267 Section 68-10. Updating the Program.

268 Upon the recommendation of the City Manager and Director of Finance, the City Council
269 shall annually review and, as deemed necessary by the Council, update the Identity Theft
270 Prevention Program along with any relevant red flags in order to reflect changes in risks
271 to customers or to the safety and soundness of the City and its covered accounts from
272 identity theft. In so doing, the City Council shall consider the following factors and
273 exercise its discretion in amending the program:

- 274 A. The City's experiences with identity theft;
275 B. Updates in methods of identity theft;
276 C. Updates in customary methods used to detect, prevent, and mitigate identity
277 theft;
278 D. Updates in the types of accounts that the City offers or maintains; and
279 E. Updates in service provider arrangements.

280 Section 68-11. Program Administration.

281 The Director of Finance is responsible for oversight of the program and for program
282 implementation. The Director of Finance is responsible for reviewing reports prepared by
283 staff regarding compliance with red flag requirements and with recommending material
284 changes to the program, as necessary in the opinion of the Director of Finance, to address
285 changing identity theft risks and to identify new or discontinued types of covered
286 accounts. Any recommended material changes to the program shall be submitted to the
287 City Council for consideration by the Council.

288 A. The Director of Finance will report to the City Manager and City Council at least
289 annually, on compliance with the red flag requirements. The report will address
290 material matters related to the program and evaluate issues such as:

291 (1) The effectiveness of the policies and procedures of City in addressing the
292 risk of identity theft in connection with the opening of covered accounts
293 and with respect to existing covered accounts;

294 (2) Service provider arrangements;

295 (3) Significant incidents involving identity theft and management's response;
296 and

297 (4) Recommendations for material changes to the Program.

298 B. The Director of Finance is responsible for providing training to all employees
299 responsible for or involved in opening a new covered account, restoring an existing
300 covered account or accepting payment for a covered account with respect to the
301 implementation and requirements of the Identity Theft Prevention Program. The Director
302 of Finance shall exercise his or her discretion in determining the amount and substance of
303 training necessary.

304 Section 68-12. Outside Service Providers.

305 In the event that the City engages a service provider to perform an activity in connection
306 with one or more covered accounts the Director of Finance shall exercise his or her
307 discretion in reviewing such arrangements in order to ensure, to the best of his or her
308 ability, that the service provider's activities are conducted in accordance with policies
309 and procedures, agreed upon by contract, that are designed to detect any red flags that
310 may arise in the performance of the service provider's activities and take appropriate
311 steps to prevent or mitigate identity theft."

312 "Article II
313 Treatment of Address Discrepancies.

314 Section 68-13. Short Title.
315 Treatment of Address Discrepancies.

316 Section 68-14. Purpose.

317 Pursuant to 16 CFR § 681.1, the purpose of this Article is to establish a process by which
318 the City will be able to form a reasonable belief that a consumer report relates to the
319 consumer about whom it has requested a consumer credit report when the City has
320 received a notice of address discrepancy.

321 68-15. Definitions.

322 For purposes of this article, the following definitions apply:

323 ‘Notice of address discrepancy’ means a notice sent to a user by a consumer reporting
324 agency pursuant to 15 U.S.C. § 1681(c)(h)(1), that informs the user of a substantial
325 difference between the address for the consumer that the user provided to request the
326 consumer report and the address(es) in the agency’s file for the consumer (*see Note 2*)

327 ‘City’ means City of Aberdeen.

328 **Note 2:** *See 16 CFR § 681.1(b).*

329 68-16. Policy.

330 In the event that the City receives a notice of address discrepancy, the City employee
331 responsible for verifying consumer addresses for the purpose of providing the municipal
332 service or account sought by the consumer shall perform one or more of the following
333 activities, as determined to be appropriate by such employee:

334 A. Compare the information in the consumer report with:

335 (1) Information the City obtains and uses to verify a consumer’s identity in
336 accordance with the requirements of the Customer Information Program rules
337 implementing 31 U.S.C. § 5318(l);

338

339 (2) Information the City maintains in its own records, such as applications for
340 service, change of address notices, other customer account records or tax
341 records; or

342 (3) Information the City obtains from third-party sources that are deemed reliable
343 by the relevant City employee; or

344 B. Verify the information in the consumer report with the consumer.

345 Section 68-17. Furnishing Consumer’s Address to Consumer Reporting Agency.

346 A. In the event that the City reasonably confirms that an address provided by a consumer
347 to the City is accurate, the City is required to provide such address to the consumer
348 reporting agency from which the City received a notice of address discrepancy with
349 respect to such consumer. This information is required to be provided to the consumer
350 reporting agency when:

- 351 (1) The City is able to form a reasonable belief that the consumer report relates to
352 the consumer about whom the City requested the report;
353 (2) The City establishes a continuing relation with the consumer; and
354 (3) The City regularly and in the ordinary course of business provides
355 information to the consumer reporting agency from which it received the
356 notice of address discrepancy.

357 B. Such information shall be provided to the consumer reporting agency as part of the
358 information regularly provided by the City to such agency for the reporting period in
359 which the City establishes a relationship with the customer.

360 Section 68-18. Methods of Confirming Consumer Addresses.

361 The City employee charged with confirming consumer addresses may, in his or her
362 discretion, confirm the accuracy of an address through one or more of the following
363 methods:

- 364 A. Verifying the address with the consumer;
365 B. Reviewing the City's records to verify the consumer's address;
366 C. Verifying the address through third party sources; or
367 D. Using other reasonable processes.

368 **Section 2**

369 The preamble to this ordinance is hereby incorporated into this ordinance as if set out
370 fully herein.

Section 3

371 All ordinances and parts of ordinances in conflict herewith are hereby expressly repealed.

Section 4

372 The adoption date of this ordinance is November 29, 2010.

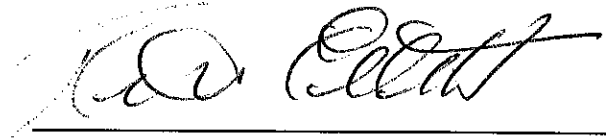
Section 5

373 The effective date of this ordinance is December 19, 2010.

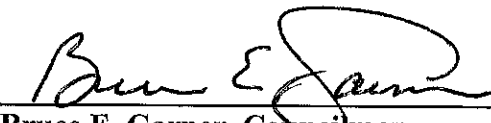
COUNCIL OF THE CITY OF ABERDEEN



Michael E. Bennett, Mayor



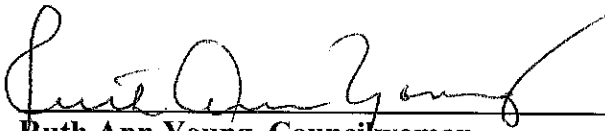
Ruth E. Elliott, Councilwoman



Bruce E. Garner, Councilman



Sandra J. Landbeck, Councilwoman



Ruth Ann Young, Councilwoman

ATTEST:

SEAL:



Monica A. Correll, City Clerk

Date November 29, 2010