

## In this issue

FACTA, the Fair and Accurate Credit Transactions Act, was enacted as an amendment to the Fair Credit Reporting Act (FCRA). The act addresses many areas of consumer data reporting. This document is an update on the following:

- Initial, extended and active-duty alerts date Oct. 15, 2004
- Implications for Notification Services
- Experian system changes — effective Oct. 15, 2004
- Address mismatch indicators
- The fifth score factor for mortgage lenders
- Medical data protection — System changes went into effect on May 14, 2004
- “Red flag” guidelines
- Frequently asked questions about FACTA

## What’s around the Legislative Corner!

### Initial, extended and active-duty alerts date Oct. 15, 2004

Experian® will deliver the initial, extended and active-duty military alerts with all credit reports as required by the FCRA. If the consumer provides a telephone number for identification verification, it will be provided with the alert.

**Initial alert (Experian’s initial security alert)** — A 90-day “temporary” alert added to a file when a consumer asserts in good faith a suspicion that he or she has been, or is about to become, a victim of fraud or a related crime, including identity theft. The consumer who adds this alert is entitled to a free copy of his or her disclosure and will be opted out of Prescreen for six months. The consumer can add a phone number to this alert so that the data user can verify the consumer’s identity. Experian will share this information with the other credit reporting agencies through the fraud exchange system already in use.

**Data user requirements** — No prospective user of a consumer report that includes an initial fraud alert may establish a new credit plan or extension of credit, other than an open-end credit plan (as defined in Section 103(i)), in the name of the consumer or issue an additional card on an existing credit account requested by a consumer or grant any increase in credit limit on an existing account requested by a consumer, unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request.

If the consumer has provided a telephone number to Experian to be used for identity verification purposes, before authorizing any new credit plan or extension of credit described above, in the name of the consumer, a user shall contact the consumer using that telephone number or take reasonable steps to verify the consumer’s identity and confirm that the application for a new credit plan is not the result of identity theft.

**Extended alert (Experian’s extended fraud victim alert)** — A seven-year alert added to a file when a consumer submits an identity theft report and proof of identity. The consumer who adds this alert is entitled to two free copies of his or her disclosure and will be opted out of Prescreen for five years. This alert must include a telephone number (or other reasonable contact method) so that the data user can verify the consumer’s identity. We are required to share this information with the other credit reporting agencies and will do so through the fraud exchange system already in use.

**Data user requirements** — No prospective user of a consumer report or of a credit score generated using the information in the file of a consumer that includes an extended fraud alert may establish a new credit plan or extension of credit, other than under an open-end credit plan (as defined in Section 103(i)), in the name of the consumer or issue an additional card on an existing credit account requested by a consumer or grant any increase in credit limit on an existing credit account requested by a consumer, unless the user contacts the consumer in person or using the contact method described (a telephone number provided to Experian or other reasonable contact method designated by the consumer) with the report to confirm that the application for a new credit plan or increase in credit limit or request for an additional card is not the result of identity theft.

**Active-duty alert (Experian’s active-duty alert)** — A 12-month alert added to a file when a consumer requests and asserts that he or she is on active duty or assigned to service away from his or her usual duty station. The consumer who adds this alert will be opted out of Prescreen for two years. Experian must share this information with the other credit reporting agencies through the fraud exchange system already in use.

**Data user requirements** — No prospective user of a consumer report that includes an active-duty alert may establish a new credit plan or extension of credit, other than an open-end credit plan (as defined in Section 103(i)), in the name of the consumer or issue an additional card on an existing credit account requested by a consumer or grant any increase in credit limit on an existing account requested by a consumer, unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request.

If the consumer has provided a telephone number to Experian to be used for identity verification purposes, before authorizing any new credit plan or extension of credit described above in the name of the consumer, a user shall contact the consumer using that telephone number or take reasonable steps to verify the consumer’s identity and confirm that the application for a new credit plan is not the result of identity theft.

### Implications for Notification Services

Beginning on Oct. 15, 2004, the Consumer Statement Indicator in your Daily Notice file will return a value of “A” if any of the above security alerts are on the file. The specific type of alert will be found in the corresponding record on the Consumer Statement file.

### Experian system changes — effective Oct. 15, 2004

Clients and vendors must code for the additional consumer statement messages to be compliant with the FCRA. Statement type 06 remains unchanged. However, clients must be able to accept the additional six new messages, numbers 26 to 31, by Oct. 15, 2004.

TTY reports: The data will appear in the Consumer Statement band; ARF versions 6 and 7: The data will appear in the 365 segment; ARF version 8: The data will appear in the 3600 segment.

| Statement type | Consumer Statement text   |
|----------------|---|
| 06             | <b>ID Fraud Victim Alert:</b> Fraudulent applications may be submitted in my name or my identity may have been used without my consent to fraudulently obtain goods or services. Do not extend credit without first contacting me personally and verifying all application information at Day XXX-XXX-XXXXEXTXXXXX or Evening XXX-XXX-XXXXEXTXXXXX. This victim alert will be maintained for seven years beginning MM-DD-YY.  |
| 26             | <b>ID Security Alert:</b> Fraudulent applications may be submitted in my name or my identity may have been used without my consent to fraudulently obtain goods or services. Do not extend credit without first verifying the identity of the applicant. This security alert will be maintained for 90 days beginning MM-DD-YY.   |
| 27             | <b>ID Security Alert:</b> Fraudulent applications may be submitted in my name or my identity may have been used without my consent to fraudulently obtain goods or services. Do not extend credit without first verifying the identity of the applicant. I can be reached at XXX-XXX-XXXXEXTXXXXX. This security alert will be maintained for 90 days beginning MM-DD-YY.   |
| 28             | <b>CRA Alert:</b> Experian has learned that information about this consumer may have been obtained without authorization, which may result in fraud. Further authentication of this consumer is recommended. This alert will be maintained on file for 180 days beginning MM-DD-YY.   |
| 29             | <b>Active-Duty Alert:</b> I am currently on active military duty. Do not extend credit without first verifying the identity of the applicant. I can be reached at XXX-XXX-XXXXEXTXXXXX. This alert will be maintained on file for one year beginning MM-DD-YY.  |
| 30             | <p><b>ID Fraud Victim Alert:</b> Fraudulent applications may be submitted in my name or my identity may have been used without my consent to fraudulently obtain goods or services. Do not extend credit without first contacting me personally and verifying all application information at Day XXX-XXX-XXXXEXTXXXXX or Evening XXX-XXX-XXXXEXTXXXXX. This victim alert will be maintained for seven years beginning MM-DD-YY.</p> <p><b>Active-Duty Alert:</b> I am currently on active military duty. Do not extend credit without first verifying the identity of the applicant. I can be reached at XXX-XXX-XXXXEXTXXXXX. This alert will be maintained on file for one year beginning MM-DD-YY.</p> |
| 31             | <b>ID Security Alert/Active-Duty Alert:</b> Fraudulent applications may be submitted in my name or my identity may have been used without my consent to fraudulently obtain goods or services. I am currently on active military duty. Do not extend credit without first verifying the identity of the applicant. I can be reached at XXX-XXX-XXXXEXTXXXXX. This alert will be maintained on file for one year beginning MM-DD-YY.   |

## Address mismatch indicators

FACTA requires that Experian notify a credit report requester if there is substantial discrepancy between the address on inquiry input and the address on file. Experian has been displaying this indicator for more than 20 years. In addition, the address mismatch indicator will be output on Quest<sup>SM</sup> and Prescreen output .

- **Data user requirements, Section 605** — The federal banking agencies, the National Credit Union Administration and the Federal Trade Commission (FTC) are establishing regulations for data users when they are notified of an address discrepancy on a consumer report. These regulations have not yet been published. However, data users should be prepared to recognize the indicator if verification procedures are mandated.
- **Experian system mismatch output indicator**  
TTY reports: Asterisk displays to the left of the address  
ARF versions 6 and 7: Segment 336, origination code 1, 4, 6 or 7  
ARF version 8: Segment 3360, origination code 1, 4, 6 or 7

## The fifth score factor for mortgage lenders

There are new requirements regarding the display of key score factors when inquiries adversely impact the score. Additionally, there are requirements on mortgage lenders to disclose this information to the consumer. Below are the software changes required to support the fifth score factor for mortgage lenders.

Experian will implement these software changes on Nov. 12, 2004.

### Which risk models will deliver the fifth score factor?

Experian will deliver the fifth score factor on all credit reports accessed on mortgage-related inquiries when one of the following risk models is requested:

| Risk model                                  | Factor code and description                              |
|---|--|
| Experian/Fair Isaac Risk Model version 1    | 08 — Number of recent inquiries                          |
| Experian/Fair Isaac Risk Model version 2    | 08 — Number of recent inquiries                          |
| Scorex PLUS <sup>SM</sup>                   | 81 — Number of recent inquiries                          |
| National Risk Model version 2               | 02 — Recent inquiries or 04 — Number of credit inquiries |
| National Risk Model version 1               | 5F — Presence of inquiries negatively impacts the score  |
| Experian/MDS Bankruptcy Model <sup>SM</sup> | 5F — Presence of inquiries negatively impacts the score  |
| Bankruptcy Watch <sup>SM</sup>              | 5F — Presence of inquiries negatively impacts the score  |

### How will a mortgage inquiry be identified?

A mortgage-related inquiry will be identified either by the Kind of Business (KOB) code associated with the inquiring subscriber code number or by the type code entered as part of the inquiry string (T-keyword).

The following KOBs will identify a subscriber code number for a mortgage-related inquiry:

| KOB | Description               |
|-----|---------------------------|
| BM  | Mortgage broker           |
| FB  | Mortgage bank             |
| FL  | Savings and loan mortgage |
| FM  | Mortgage company          |
| FR  | Mortgage reporter         |

The following purpose type codes will be considered mortgage related:

| Type code | Description                            | Type code | Description                                      |
|-----------|--|-----------|--|
| 04        | Home improvement loan                  | 2C        | FMHA real-estate (Farmers Home Administration)   |
| 05        | FHA home improvement loan              | 5A        | Real estate — junior liens and nonpurchase money |
| 08        | Real-estate loan                       | 5B        | Second mortgage (terms in years)                 |
| 0A        | Time-share loan                        | 6B        | Commercial mortgage loan                         |
| 16        | FHA co-signer                          | 6D        | Home-equity installment loan                     |
| 17        | Manufactured home                      | 85        | Bimonthly mortgage payment                       |
| 19        | FHA mortgage                           | 86        | Automated mortgage report                        |
| 25        | VA real-estate mortgage                | 87        | Semimonthly mortgage payment                     |
| 26        | Conventional real-estate mortgage      | 9A        | Secured home improvement loan                    |
| 27        | Real-estate mortgage (terms in months) |           |  |

### Where will the fifth score factor display?

A new message number has been assigned to identify this message as being the fifth score factor. The model identifier, score factor code and the score factor description will be present in this message. If multiple models are requested, the delivery of the fifth score factor in the TTY message band or ARF segments will be in the same order as the scores and other factor codes are displayed in the TTY score band, 125, 130 or 1250 ARF segments.

For teleprinter (TTY human readable) reports, the fifth score factor will display in the message band at the bottom of the report.

### TTY example:

----- MESSAGES -----

MSG 335: B 5FPRESENCE OF INQUIRIES NEGATIVELY IMPACTS THE SCORE

For ARF versions 6 and 7 — This message will display in the 361-message segment.

### Example of the 361 segment:

| 361 message — segment |        |          |           |  |
|-----------------------|--------|----------|-----------|--|
| Field name            | Length | Position | Data type | Value  |
| Record ID             | 3      | 1–3      | N         | 361  |
| Record length         | 4      | 4–7      | N         | 42   |
| Message number        | 2      | 8–9      | N         | 57   |
| Text length           | 2      | 10–11    | N         | 30   |
| Message text          | 1–99   | 12+      | A/N       | 0335B 5FPRESENCE OF INQUIRIES NEGATIVELY IMPACTS THE SCORE |
| End segment mark      | 1      | +13      | A/N       | @  |

Display in the 361 segment in the Credit Report output:

361007157590335 B 5FPRESENCE OF INQUIRIES NEGATIVELY IMPACTS THE SCORE@

For ARF version 08 — This message will display in the 3610 message segment.

### Example of the 3610 segment:

| 3610 message — segment |        |          |           |   |
|------------------------|--------|----------|-----------|---|
| Field name             | Length | Position | Data type | Value   |
| Record ID              | 4      | 1        | N         | 3610  |
| Record length          | 4      | 5        | N         | 38  |
| Message code           | 4      | 9        | N         | 0335  |
| Length of message text | 4      | 13       | N         | 30  |
| Message text           | 0–9999 | 17       | A/N       | B 5F PRESENCE OF INQUIRIES NEGATIVELY IMPACTS THE SCORE |
| End of segment mark    | 1      |          | A/N       | @   |

Display of the 3610 segment in the Credit Report output:

3610007103350054B 5FPRESENCE OF INQUIRIES NEGATIVELY IMPACTS THE SCORE@

### Medical data protection — System changes went into effect on May 14, 2004

FACTA establishes restrictions on sharing medical information. The definition of medical information now includes medical payment information. The effective date of Experian's new requirement was June 4, 2004. To ensure compliance, Experian is making the following changes.

- Medical information appearing in the subscriber name field and/or the original creditor field on collection accounts or in the plaintiff name field on public record data will be edited on output and display with the generic term "Medical payment data."
- The name of any direct reporters of medical data (KOB "M") will display with the generic term "Medical payment data."
- The subcode of direct reporters of medical data (KOB "M") will be protected from the "decode" process. An error message will be received if the decode process is requested on these specific subcodes.
- Consumer disclosures will continue to display the actual original creditor name, plaintiff name and direct reporter name. However, copies of a revised disclosure sent to a client will have the data modified as stated above.

Clients and vendors are not required to make any software changes on this information, as only the verbiage of the output data is being modified.

There are, however, provisions in FACTA, effective early in 2005, that require furnishers of medical information to use codes to identify the data being provided to Experian and the other credit reporting agencies. The Metro 2 format has a "Creditor Classification" field that, if used, ensures compliance with this client requirement. A letter from the CDIA has been sent to all medical data furnisher clients urging them to begin using Metro 2 and the "Creditor Classification" field as soon as possible.

### "Red flag" guidelines

The federal banking agencies, the National Credit Union Administration and the FTC are establishing new regulations and guidelines to identify and prevent possible identity theft. Among the patterns and practices being studied are address changes and inactive account handling. These regulations have not yet been published; therefore, we can offer no information at this time.

### Frequently asked questions about FACTA

#### 1 What percentage of the consumer file contains or is projected to contain these types of alerts?

Today on File One<sup>SM</sup> we have approximately 200,000 extended alerts and approximately 580,000 initial alerts.

#### 2. Have all of these initial or extended alerts occurred since FACTA was enacted or does this include prior fraud victim alert history?

FACTA requirements for alerts do not go into effect until Dec. 1, 2004. All the on-file alerts today are pre-FACTA and will remain on file and roll into the FACTA requirements.

#### 3. What are your plans regarding existing fraud victim alerts? Will they be converted to appear in the new FACT Act form or will these original forms still be appearing?

The extended alerts will continue to display as statement 06; all others will be converted to the new types.

**4. What is a CRA alert and how does it differ from the other types of alerts included? Is it characterized as either an initial alert or an extended alert or something else entirely?**

The CRA alert is not consumer initiated. This alert is added to a file when Experian has been notified by another source that there has been a security breach and consumer identification information was compromised. This alert is added to the file and should be treated as something similar to an initial alert. This alert is on file for six months. If the consumer contacts Experian, we will delete the CRA alert and add a fraud alert if the consumer requests it. The fraud alert could be either initial or extended, depending on the consumer request.

**5. What is the difference between a security alert and a fraud victim alert in your coding?**

The security alert is now referred to as the initial alert. The fraud victim statement is now referred to as the extended alert.

**6. It appears that you are defining all current fraud victim alerts to be comparable with extended alerts. Is that correct? What is the difference today (pre-FACTA) between the security alert and the fraud alert process? There are several messages that are considered fraud alerts.**

The extended alert was formally called the fraud victim statement, and the initial alert was formally called the security alert. Our processing remains the same to add these alerts to a file. The only difference in processing with FACTA is that we will require an identity theft report before adding the extended alert to a consumer file.

**7. What is your process for establishing an active-duty alert?**

Consumers will make the request through our National Consumer Assistance Center Interactive Voice Response process, which allows the alert to be placed in a file immediately.

**8. What is the NCAC IVR (National Consumer Assistance Center Interactive Voice Response) process? Does the consumer need to provide any documentation? Can someone else put the alert on for the consumer (e.g., a spouse)?**

A consumer can call the National Consumer Assistance Center Interactive Voice Response to add an initial alert or the active-duty alert. The consumer is processed through our authentication process before he or she is granted access to the data.

**9. In establishing alerts, how will you handle sequential contact information? Will you resolve discrepancies? For example, if there is an existing fraud victim alert containing phone number 222 222 2222 and after Jan. 1, 2005, there is a new extended or active-duty alert with contact phone number 333 333 3333, will both contact directions remain on the consumer's file or will you resolve the consumer's choice of contact when you add the new alert so there is only one contact point identified?**

The consumer can add only one type of fraud message to his or her file at a time. The active-duty alert can be added at any time, as it is not the same as a fraud alert. If the consumer has added an extended alert and needs to update the phone number, we will accommodate that update. If the consumer has added an extended alert and then an active-duty alert with different phone numbers, we will include the phone numbers with each statement.

**10. What percentage of the alerts will contain a phone number?**

Today only the extended alerts can add phone numbers. There currently are 200,000 on file with a phone number. FACTA provides the ability to add phone numbers with the initial alert. Since we have no initial alerts on file today with a phone number, we have no base line to create this estimate.

**11. What other contact information would you be providing within the alert message — for example, multiple phones, e-mail address, postal address, personal representative name or other?**

None. At this time, Experian will be adding only phone numbers for this contact.

**12. It appears that certain state-type regulations may provide incremental benefits to the consumer in addition to FACTA requirements. When you receive a state-type alert, will it be encoded exclusively as that state level or will it also be encoded as FACTA? For example, will California identity theft appear exclusively as California identity theft or will it also have initial/extended alert flags?**

All the alerts will be added per the FACTA requirements.

**13. If a consumer has an initial alert and subsequently meets the conditions for an extended alert, will both alerts be contained on the file or will only the extended alert remain?**

Both alerts will be maintained in the file and displayed as a combination message.

**14. I didn't see any combination message for initial alert and extended alert. Which message is supposed to have that condition?**

There are only combination messages when one of the on-file alerts is the active-duty alert. If there is no active-duty alert, then we will display the alert most recently added to the file.

**15. Today, Notification Services provides a security trigger on accounts. What exactly would be added to the consumer file that would activate this security trigger?**

There are four different initial alerts that Notification Services will trigger upon:

1. Initial alert/No phone
2. Initial alert/With phone
3. Active-duty alert
4. CRA Alert Message

When a consumer has been a victim of fraud and contacts Experian, the initial alert is added to the file immediately. This alert is maintained on the file for 90 days. The addition of this alert on the file will produce a trigger from the Notification Services system.

A consumer on active military duty may add the active-duty alert to his or her file. This also will be done via phone and will be added to the file immediately. The addition of the alert to a file will produce a trigger from the Notification Services system.

If a client contacts Experian and reports a breach of security where consumer identification information was compromised, we will add the CRA Alert to the file immediately. The addition of this alert will produce a trigger from the Notification Services system.

The Notification Services output will contain an indicator advising you of the presence of the fraud alert; the full text message is provided in a separate file that contains the full credit report output.

The extended alert is added to a file only after the consumer has contacted Experian and provided us with an identity theft report. All extended alerts are preceded by an initial alert; therefore, we do not provide a trigger for the extended alert.

---

**Provided to you compliments of Experian. For more information, please contact your local Experian representative.**

Experian is a global leader in providing information solutions to organizations and consumers. We help organizations find, develop and manage profitable customer relationships by providing information, decision-making solutions and processing services. We empower consumers to understand, manage and protect their personal information and assets. Experian works with more than 40,000 clients across diverse industries, including financial services, telecommunications, health care, insurance, retail and catalog, automotive, manufacturing, leisure, utilities, property, e-commerce and government. Experian is a subsidiary of GUS plc and has headquarters in Nottingham, UK, and Costa Mesa, Calif. Our 13,000 people support clients in more than 60 countries. Annual sales exceed \$2.2 billion.

