



TRANSUNION WHITE PAPER

Red Flags: Gaining Perspective on New Identity Theft Prevention Regulations

By Charles Deremer, Senior Business Consultant, TransUnion Fraud and Identity Management Solutions

1 Introduction

2 What are Red Flags and how do they affect financial institutions?

3 Rising consumer credit creates a strong need for effective identity management and fraud prevention

4 Building an effective identity management approach

8 Managing potential fraud

9 Helping ensure more effective identity management

10 Appendix A – Examples of Red Flags

This White Paper was not prepared by an attorney and may not reflect the opinions of the TransUnion Law Department. The information contained in this White Paper is not intended as and in no way constitutes legal guidance and/or advice of any nature from TransUnion, nor is anything contained herein a guarantee that your fraud and identity management program will be compliant with Red Flag Regulations. TransUnion makes no warranties of any kind concerning the information provided in this White Paper. You must consult your own legal counsel or compliance advisor to determine whether your fraud and identity management programs will enable your organization to meet your compliance obligations associated with Red Flag Regulations.

© 2007 TransUnion LLC. All Rights Reserved

No part of this publication may be reproduced or distributed in any form or by any means, electronic or otherwise, now known or hereafter developed, including, but not limited to, the Internet, without the explicit prior written consent from TransUnion LLC.

Requests for permission to reproduce or distribute any part of, or all of, this publication should be mailed to:

Law Department
TransUnion
555 West Adams
Chicago, Illinois 60661

The “T” logo, TransUnion, and other trademarks, service marks, and logos (the “Trademarks”) used in this publication are registered or unregistered Trademarks of TransUnion LLC, or their respective owners. Trademarks may not be used for any purpose whatsoever without the express written permission of the Trademark owner.

Introduction

According to a Gartner study released in February 2007, identity theft has increased 50% from 2003 through 2006 and more than 15 million Americans were victims of identity-theft related fraud in 2006.¹ While there is debate within the industry whether identity theft is actually increasing, the impact of identity theft on regulatory perception is clear. In July 2006, the national financial institution regulatory agencies and the Federal Trade Commission proposed new guidelines generally referred to as the Red Flag Regulations that would require financial institutions to develop and maintain a comprehensive identity theft prevention program.

The final Red Flag Regulations were released on October 16, 2007 and are outlined in a 256-page report. While the regulations are broad in scope, TransUnion offers a full suite of fraud and identity management solutions that can help financial institutions and creditors address certain regulatory obligations, including:

Establishing written policies and procedures for preventing, detecting and responding to identity theft.

Developing and applying reasonable policies and procedures to verify change of address requests and notifications.

Maintaining and updating policies and procedures to respond to evolving identity theft trends within the organization.²

Financial institutions must ensure compliance with the current requirements by November 1, 2008. Apart from any regulatory requirements you may have, protection against identity theft is important for business reasons as well. The Federal Register “Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003: Final Rule” was used as a general guideline in the writing of this document, located at: <http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf>.

What are Red Flags and how do they affect financial institutions?

One outcome of the Red Flag Regulations is to establish a foundation that would effectively reduce the frequency and impact of identity theft. The regulations include 26 illustrative examples of Red Flags associated with potential identity theft (see Appendix A).

For purposes of the regulation, Red Flags are a pattern, practice or specific activity that indicates the possible risk of identity theft. The Red Flags can be categorized into the following areas:

Alerts, notifications or warnings from a consumer reporting agency

Suspicious documents

Suspicious personal identifying information

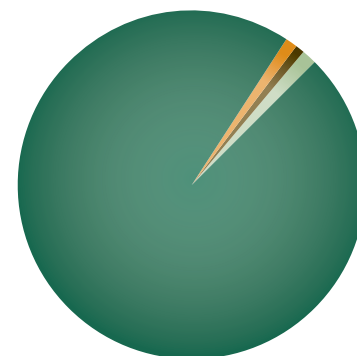
Unusual use of, or suspicious activity related to, a covered account

Notice from consumers, victims of identity theft, law enforcement authorities or other persons regarding possible identify theft in connection with covered accounts held by the financial institution or creditor

The Red Flag Regulations provide 26 examples of activities that may indicate potential identity theft with new and existing accounts. These examples can be primarily categorized as account or relationship origination and account management.³

Financial services continue to be the primary target of phishing and pharming attacks as demonstrated in Figure 1. These attacks increase the potential risk of account takeover and support recent reports released by Javelin Strategy and Research. Now more than ever, financial institutions and creditors must take reasonable steps to verify each consumer and validate that the request is authentic. These steps must be comprehensive, documented and clearly identify monitoring and response approaches.

FIGURE 1
Most Targeted Industry Sectors in May 2007



Financial Services 96.9%
ISP 1.2%
Government and Miscellaneous 1.2%
Retail 0.8%

Source: Anti-Phishing Working Group⁴

The financial services industry receives the majority of phishing and pharming attacks.

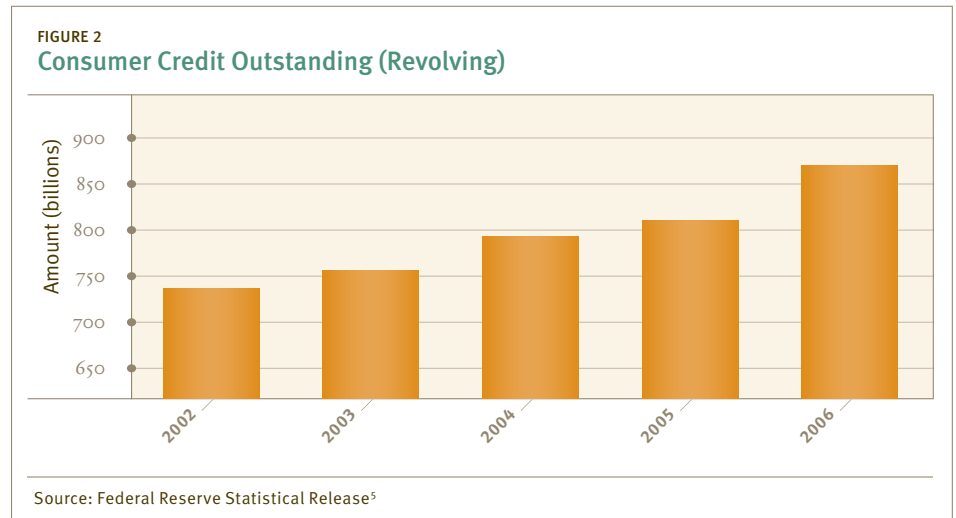
Rising consumer credit creates a strong need for effective identity management and fraud prevention

Consumer credit has been steadily increasing over the past several years. According to the Federal Reserve Statistical Release on April 5, 2007, consumer credit outstanding stands at approximately \$880 billion (see Figure 2).

Consumer credit trends indicate the potential demand for credit services and help explain the concern of regulators. Verification is critical to maintaining the significant and increasing levels of consumer credit. Effective verification of consumer identity is critical to reducing identity theft. However, the process for verification is complex and multi-dimensional, and there are no universal standards for identity verification. There is a critical need for stronger verification.

Identity verification is the process of verifying the indicative information provided by the consumer. This may occur at various points in the customer lifecycle, including:

- Issuance of authority or credentials
- Establishing a relationship
- Managing the relationship



Outstanding consumer credit has grown steadily since 2002.

Each area relates to the others, providing a support framework. Therefore, a common approach to identity verification should be implemented at every step. A breakdown in any one area increases

the potential risk of identity theft. There are known deficiencies within each area that allow identity theft to proliferate.

Building an effective identity management approach

Typically, authorization or credentials are granted after a defined verification process. However, identified gaps in the process have enabled identity manipulation and theft. As a result, financial providers lose confidence in the documents required to prove identity. An efficient, secure identity verification approach must consider this confidence factor and continue to ensure accuracy.

The effective identity management process must be dynamic and must include a structured framework consisting of:

Flexible approach. The identity management framework must be flexible, maintaining the ability to adapt to changes in data, functionality, technology and volume. The approach must be able to incorporate third-party data as well as new technology that may be required to meet the needs of evolving products, services and compliance issues.

Quality data. The framework collapses without access to and effective use of quality data. Multi-sourced data provides the most complete coverage and best potential for verifying the indicative information provided. Multiple sources can include several internal databases, external credit files and access to numerous non-credit data sources.

Verification. Verification is the validation and authentication of the consumer and/or the data provided by the consumer against known, trusted sources. In this step, the organization reviews the validity of the data and matches data against known information and identifies inconsistent, inaccurate and potentially fraudulent information.

Authentication. In some cases, verification of known data may not sufficiently prove identity.

Authentication provides an additional level of assurance. Authentication is the recognition and affirmation of personal identifiers. It also recognizes the financial institution's relationship with the consumer.

Access to quality data

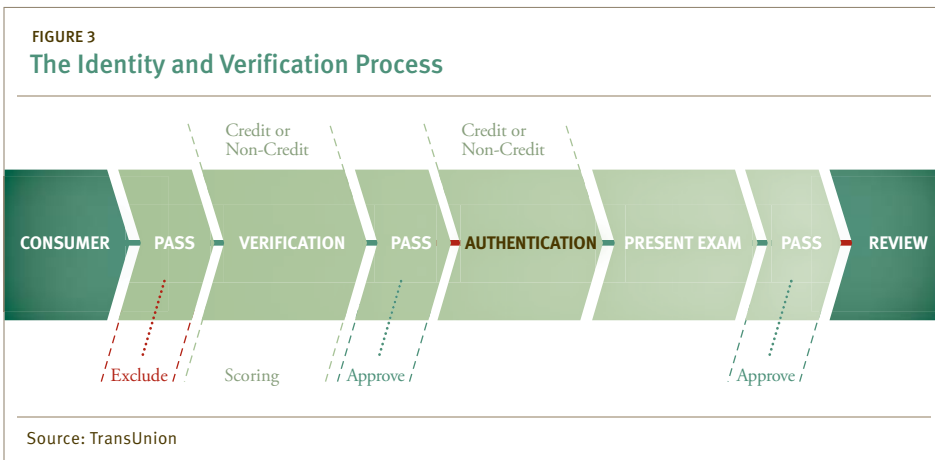
Effective identity management requires accurate, reliable and secure information. The data may be internal or external, but must provide a reasonable assessment of the risk associated with the request. The types of data that may be referenced should be based on the nature of the request and the risk associated. Low-risk activities may rely strictly on internally available data, while more risky activities trigger access to external sources.

Establishing a new relationship with a previously unknown consumer requires some level of assurance to protect the consumer and institution. Assurance is developed by evaluating the available information concerning the consumer. However, the information must reflect

an accurate profile. Credit Reporting Agencies maintain timely data on millions of consumers and remain one of the leading sources of data for financial institutions and creditors. In addition to having one of the largest raw data sources on consumers, the credit reporting agencies further provide solutions that transform the data into useful information organizations can use to make more informed business decisions.

Verification and authentication to establish a new relationship

Most financial institutions and creditors have implemented guidelines and procedures for identifying and responding to potential cases of identity theft. Good practices specifically focus on reasonable policies and procedures to validate address discrepancies and changes, particularly where there is a difference with data provided by a consumer credit reporting agency. Generally this process is already in place, as most financial institutions and creditors process credit



This process flow diagram shows an effective, integrated approach to identity verification and authentication.

data at application and at various points in the customer relationship (Figure 3).

The identity management process is initiated when a consumer attempts to establish a relationship. The indicative information provided by the consumer is screened for initial validity. If the consumer fails initial checks (excessive attempts, incomplete or insufficient data), the request is excluded. When

the initial identity criteria are met, the indicative information is validated. Validation ensures that the information provided meets known standards such as formatting and issuance. Valid indicative information is then verified against credit and non-credit data sources as well as negative databases. Data sensibility checks further ensure that the information provided is reasonable and logical for the consumer. Positive

verification against multiple data sources provides a reasonable level of assurance related to the identity of the consumer.

A component of the verification process is the relational scoring of the indicative information. A fraud score assesses the various indicative data and provides a numerical representation of the risk associated with a consumer. The score takes into consideration known fraud patterns and data as well as the overall validity of information provided. An additional score gaining support is the Identity Score. This score assesses the various patterns within the identity data and provides a numerical representation of the risk associated with the indicative information presented.

Consumers matching known fraud profiles are excluded from further consideration. Consumers failing verification, but not meeting the expectation of fraud, are eligible for authentication. Consumers are presented

with an out-of-wallet exam based on the consumer credit and non-credit data on file. The consumer is asked a set of questions that only he/she should know. The successful completion of the exam demonstrates a reasonable level of confidence in the identity of the consumer.

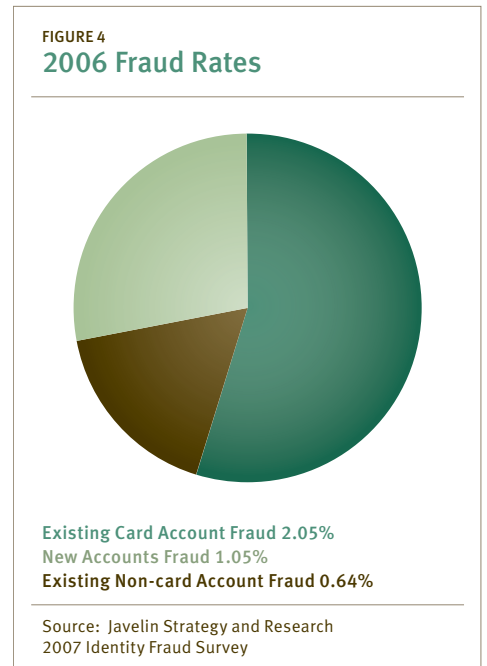
Only through a comprehensive verification of the consumer can identity be assured. Merely providing physical documentation is not sufficient to prove identity at any stage of the process. The indicative information contained with the documentation must be verified against the additional data provided by the customer and trusted third-party data sources.

Verification and authentication in account management

Identity verification and authentication is not a point solution, but a process. It is no longer sufficient to screen a consumer at the beginning of a credit relationship and not reassess risk at various points in the lifecycle. The process must be revisited at various points throughout the relationship with the consumer. The Red Flag Regulations provide numerous examples of account usage-based indicators of identity theft.

Fraud involving established accounts appears to be the most commonly reported fraud trend in the financial services industry. In fact, unauthorized activity on existing accounts was the most common fraud type reported in the Javelin 2007 Identity Theft Survey (see Figure 4).⁶

Many financial institutions and creditors have risk-based account monitoring tools to identify anomalous account behavior.



Unauthorized changes on accounts can indicate the first step in potential fraud.

However, a more structured and comprehensive approach is the better strategy. Changes to the indicatives on the account, such as address change requests, new contact numbers and

new authorized users, should be quickly verified against trusted data sources to confirm validity.

The most effective approach to reducing the risk of fraudulent usage is to prevent the opening of new fraudulent accounts or the fraudulent takeover of existing accounts. Preventing fraudulent account creation is accomplished by thoroughly screening account-based indicatives. However, even with best practices implemented on the front end, fraud is likely to occur on the back end. Usage anomaly detection tools exist that effectively identify potential fraudulent behavior. Usage monitoring or profiling is one of the more common approaches to managing fraud during the account management period.

Usage fraud is an evolving target. Fraudulent usage patterns and details consistently shift as fraudsters learn detection techniques. Even with comprehensive front- and back-end

fraud management tools, a significant amount of fraud remains undetected within most organizations. Additional approaches are necessary to supplement usage monitoring. Patterns of credit usage may be indicative of fraud. When financial providers can access timely, comprehensive, third-party data, they can better identify those patterns.

A global or industry view is necessary to capture the potential for organized fraud. Patterns of fraud and abuse will be reflected in risk scores associated with the consumer. Fraud is rarely isolated to a singular occurrence or to one target. A holistic view of fraud across the business and across the industry will identify potential high-risk accounts. Fraud or identity scoring provides increased detection capabilities by dynamically analyzing attributes over time.

Additional root-cause analysis could help financial institutions detect fraud among existing account holders and monitor for

changes to the overall fraud risk within the account portfolio. Specific fraud messages could be provided that are indicative of fraud, such as a change of address or change in credit score. Identity management and fraud prevention experts with experience in the financial services industry can help providers create or modify fraud strategies, processes and procedures to reduce the risk of fraudulent usage.

Managing potential fraud

Fraud may occur regardless of the anti-fraud best practices in place. Identifying potential fraud includes monitoring for anomalous usage and account behavior. Each area is specifically categorized in the proposed regulation.

It's estimated that two-thirds of account takeover fraud can be attributed to fraudulent change of address.⁷ Typically, address changes processed immediately prior to a new request for service or products can be a strong indicator of fraud. Processes and monitoring systems should be configured to capture higher risk changes to an account, including address changes.

Address changes can and should be verified against external third-party sources. External sources must be current and accurate in order to reduce false positives associated with older aggregated data. Anomalous usage is one of the primary detection methods incorporated in financial services as well as most other industries. Significant changes in the use of the account, such as a dramatic shift in spending or payment patterns, indicates a change in the consumer account profile and may be a precursor to fraud losses.

Financial institutions have tools and procedures in place to identify anomalous usage related to existing accounts, and this can be effective. However, preventing the opening of new fraudulent accounts from the beginning is even more effective—in effect, preventing fraud right at the start.

The fraud management and response program should include procedures to manage external notification or alerts. External sources may include other financial institutions or businesses, credit reporting agencies or consumers. Alerts may relate to non-receipt of regular documentation, suspect emails or websites, or a report of identity theft. Financial institutions have policies and procedures in place to manage phishing and pharming fraud. This relationship should and has been expanded recently. For example, when a financial institution is notified that a consumer has been the victim of a phishing or pharming

scheme, the financial institution offers protective measures such as providing a new card number or password, establishing a fraud alert and providing credit monitoring to protect the consumer.

Consumer notification may be required when fraud is identified on an account. The credit reporting agencies may be notified by the consumer when fraudulent accounts or transactions are identified. Typically, the effective response to an identified fraud requires support from the financial institution and the consumer. The consumer should scrutinize his consumer credit report to identify and resolve additional fraudulent activity that may be present on his consumer credit file.

Helping ensure more effective identity management

The goal of an effective identity management program is to provide a reasonable level of assurance and trust for both financial providers and consumers. In some cases, those consumers passing verification are presented for authentication. Financial institutions can achieve the strongest confidence level in identity management when a consumer successfully passes both verification and authentication.

An effective approach to identity management also will support all applicable, multidimensional legal requirements and regulations, such as Red Flags, Federal Financial Institutions Examination Council (FFIEC) Multifactor Authentication, the USA PATRIOT ACT, the Office of Foreign Assets Control (OFAC) and The Fair and Accurate Credit Transactions Act (FACTA). In addition, this approach should meet these high-level business requirements:

Mitigating fraud losses

Reducing operational costs

Improving quality

There is no panacea for identity management in financial institutions. Effective mitigation will require the use of new technologies and approaches within the existing fraud prevention policy. Identity management must be integrated within the business process. A strong consumer authentication will support numerous technologies and account management best practices. By securing the beginning of a new credit relationship, financial institutions and creditors are better able to manage security throughout the lifecycle. A comprehensive fraud management program can mitigate losses and improve the relationship between financial institutions and consumers.

APPENDIX A

Examples of Red Flags

These examples of Red Flags have been summarized from “Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003,” pages 89-90.⁸

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1	A fraud or active duty alert is included with consumer report.
2	A consumer reporting agency provides notice of a credit freeze in response to a request for a consumer report.
3	A consumer reporting agency provides a notice of address discrepancy.
4	A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity for an applicant or consumer, such as: <ul style="list-style-type: none"> a. Recent and significant increase in the volume of inquiries. b. An unusual number of recently established credit relationships. c. A material change in the use of credit, especially with respect to recently established credit relationships. d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5	Documents provided for identification appear to have been altered.
6	The photograph or physical description on the identification is not consistent with the appearance of the applicant or consumer presenting identification.
7	Other information on the identification is not consistent with information provided by the person opening a new account or consumer presenting the identification.
8	Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9	An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10	Personal information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example: <ul style="list-style-type: none"> a. The address does not match any address in the consumer report; or b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration’s Death Master File.
11	Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
12	Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by financial institutions or creditors. For example: <ul style="list-style-type: none"> a. The address on an application is the same as the address provided on a fraudulent application; or b. The phone number on an application is the same as the number provided on a fraudulent application.
13	Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: <ul style="list-style-type: none"> a. The address on an application is fictitious, a mail drop, or prison; or b. The phone number is invalid, or is associated with a pager or answering service.

APPENDIX A (continued)

Suspicious Personal Identifying Information (Continued)

14	The SSN provided is the same as that submitted by other persons opening an account or other customers.
15	The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16	The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17	Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18	For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19	Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional or replacement cards or cell phone, or for the addition of authorized users on the account.
20	A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example: a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or, b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21	A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: a. Nonpayment when there is no history of late or missed payments. b. A material increase in the use of available credit. c. A material change in purchasing or spending patterns. d. A material change in electronic fund transfer patterns in connection with a deposit account. e. A material change in telephone call patterns in connection with a cellular phone account.
22	A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23	Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24	The financial institution or creditor is notified that the customer is not receiving paper account statements.
25	The financial institution or creditor is notified of unauthorized charges in connection with a customer's covered account.

Notice from Consumers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditors

26	The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
----	---

Red Flags: Gaining Perspective on New Identity Theft Prevention Regulations

¹ *Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003*. Gartner, Inc. February 28, 2007. <http://www.gartner.com/it/page.jsp?id=501912> (accessed August 20, 2007).

² Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); Office of Thrift Supervision, Treasury (OTS); National Credit Union Administration (NCUA); and Federal Trade Commission (FTC or Commission). *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003*. <http://www.ftc.gov/os/2007/10/r611019redflagsfrn.pdf> (accessed November 26, 2007).

³ Ibid.

⁴ *Phishing Activity Trends Report for the month of May 2007*. Anti-Phishing Working Group. Released July 8, 2007. http://www.antiphishing.org/reports/apwg_report_may_2007.pdf (accessed August 20, 2007).

⁵ Federal Reserve Statistical Release. *Consumer Credit February 2007*. Released April 6, 2007.

⁶ Monahan, Mary T. 2007 *Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary*. Javelin Strategy and Research. Page 9. February 2007.

⁷ Ibid.

⁸ *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003*.



TransUnion®

© 2007 TransUnion LLC
All Rights Reserved
555 West Adams Street
Chicago, Illinois 60661
USA

transunion.com/business