Counseling Identity Theft Victims

Identity theft is an American criminal epidemic that is rendering obsolete the old adage "crime doesn't pay."

By Chad Baruch*

Identity theft does pay, and it pays well. Recent surveys indicate that identity theft is one of the fastest-growing crimes in the United States, affecting millions of Americans each year.[1] In response to the proliferation of identity theft, the Texas and federal governments recently enacted provisions to assist victims of identity theft.[2] This article briefly reviews these new laws and provides information to attorneys on counseling identity theft victims.

I. Identity Theft: What It Is and How It Happens

Identity theft is the fraudulent use of another person's identity or credit history for financial gain.[3] Some of the most common types of identity theft include:

- using or opening a credit card account fraudulently,
- opening a telecommunications or utility account fraudulently,
- using or opening a bank account fraudulently (including passing bad checks), and
- obtaining loans in another person's name or by using another person's credit history.[4]

Common warning signs of identity theft include:

- credit card statements showing purchases the consumer did not make,
- credit card statements for cards the consumer did not seek,
- missing checks,
- bank and credit card statements that arrive later than normal, and
- being rejected for a loan or credit card when the consumer's credit history should support it.[5]

There are a variety of means by which identity theft is accomplished. Among the more common methods of identity theft are rifling through discarded trash, stealing from desks in the workplace, stealing mail, pretext calling,[6] fraudulent letters offering non-existent prizes or investment opportunities,[7] and phishing.[8]

Identity theft exacts a tremendous toll on American consumers. In addition to the cost in both money and time to its victims, estimates place the annual cost to American business in the billions of dollars.[9] This cost, like any significant cost in a marketplace economy, is eventually passed back to consumers.

II. New Identity Theft Provisions: Texas Law

Effective September 1, 2003, Texas has new provisions designed to assist victims of identity theft.[10] Texas is now one of a handful of states that permit identity theft victims to block access to their credit reports unless they personally unlock the reports by contacting the credit bureaus and providing a personal code or password. This is accomplished by two statutory creations, the security alert and security freeze.[11]

A. The Texas Security Alert

The purpose of the Security Alert is to assist consumers who believe, but are not certain, that they have been the victims of identity theft. A Texas consumer may request, either in writing or by telephone (and upon providing proper identification), that a temporary security alert be placed on the consumer's file not later than twenty-four hours after the consumer reporting agency receives the request.[12] This security alert must remain in effect for at least forty-five days.[13] At the end of the temporary alert period, and upon request by

the consumer, the consumer reporting agency must provide the consumer with a copy of the consumer's file. A consumer may in connection with requesting the security alert provide a telephone number to be used by persons to verify the consumer's identity before entering into transactions with that consumer.[14] Upon placement of a security alert, the consumer reporting agency is required to notify all persons requesting the consumer's report of the security alert, and include the verification telephone number if it has been provided by the consumer.[15]

Consumer reporting agencies are now required to maintain a toll-free telephone number for the purpose of fielding security alert requests; this telephone number must be answered during normal business hours and have an automated answering system after normal business hours.[16] Consumer calls taken after hours must be returned the following business day.[17]

B. The Texas Security Freeze[18]

Texas law also permits placement of a security freeze on a consumer file.[19] This procedure, however, is available only to consumers who can establish that they have been the victims of identity theft.[20] A security freeze request must be made by certified mail, and must include both proper identification and a valid police or investigative report establishing an actual identity theft. [21] Within five business days after receipt of such a request, a consumer reporting agency is required to place a security freeze on the consumer's file.[22] The consumer reporting agency also must disclose to the consumer the process of placing, removing, and temporarily lifting that security freeze, and the process for allowing access to information from the consumer's file to a particular requester while the security freeze is in effect.[23]

A consumer reporting agency must send written confirmation of the security freeze to the consumer and provide a unique code or password to authorize removal or temporary lifting of the security freeze within ten business days of receiving a consumer's proper request.[24] A consumer may then request and obtain a replacement code or password.[25] A consumer reporting agency may impose a modest fee for placing a security freeze.[26]

Once a security freeze is in effect, a consumer reporting agency must notify the consumer of any material change to the consumer's name, date of birth, social security number, or address within thirty calendar days of making the change.[27] The consumer reporting agency must also notify all persons requesting the consumer's report that the security freeze is in effect.[28] After obtaining a security freeze, the consumer may have it removed or temporarily lifted for a specified period of time or certain requestor.[29] The consumer reporting agency may not charge the consumer for doing so.[30] A consumer reporting agency is required to remove any security freeze placed as the result of a consumer's material misrepresentation, but must notify the consumer in writing prior to doing so.[31]

There are a number of exemptions from the security freeze provision, including consumer reports provided to governmental entities under a subpoena or court order, furnished to child support agencies in connection with collection of child support, requested by the comptroller or a tax assessor in connection with attempts to collect delinquent taxes, a person prescreening under the Fair Credit Reporting Act, or a person with whom the consumer already has an account or contract (so long as the request is made in connection with that existing contract or account), certain situations involving the investigation of fraud, and other limited circumstances.[32]

All consumer reporting agencies are required to honor a security freeze placed by another consumer reporting agency.[33] Perhaps most important to practitioners is the fact that any violation of the security alert or security freeze provisions is now deemed a deceptive trade practice and is actionable under the Texas Deceptive Trade Practices Act.[34]

One of the more significant changes under FACTA is that for the first time, consumers are permitted to dispute the accuracy of information directly with furnishers.[56]

III. New Identity Theft Provisions: Federal Law

The Fair Credit Reporting Act (known as the FCRA) was enacted in the 1970's, and was designed to regulate consumer credit reporting.[35] In 2003, the FCRA was amended by the Fair and Accurate Credit Transactions Act (often referred to as the FACT Act or FACTA).[36] A number of these 2003 amendments were designed to assist the victims of identity theft.[37] Most FACTA provisions were effective as of December 1, 2004.[38]

Under FACTA, a consumer may require that a consumer reporting agency place a fraud alert on the consumer's file, which the agency must then report to other consumer reporting agencies.[39] The alert notifies users of consumer reports not to extend or increase credit without first taking steps sufficient to verify the consumer's identity.[40] Additionally, furnishers of credit information must have reasonable procedures in place to respond to notice of information blocked due to identity theft, and if furnished with an identity theft report must stop furnishing that information.[41] There are two primary types of fraud alerts under FACTA, known as an initial "one-call" alert and an extended fraud alert.[42]

A. The Initial "One-Call" Alert[43]

A consumer who suspects in good faith that the consumer has been or is about to become the victim of identity theft may direct a consumer reporting agency to include a fraud alert in the consumer's file. [44] This fraud alert must be provided to anyone obtaining the consumer's file for a period of not less than ninety days, unless the consumer requests its removal during that period. The initial fraud alert is termed a "one-call" alert because the consumer reporting agency receiving it is required to convey it to the other consumer reporting agencies. The consumer may also in this circumstance obtain a free copy of the credit report.[45] Like the Texas Security Alert, this alert is designed for individuals who believe, but are not certain, that they have been the victims of identity theft.

B. The Extended Fraud Alert[46]

An extended fraud alert is available to a consumer who submits an actual identity theft report.[47] Unlike the initial alert, an extended fraud alert is available only to persons who are certain they have been the victims of identity theft. To obtain the extended fraud alert, a consumer must file an official identity theft report with a law enforcement agency.

An extended fraud alert remains active in the consumer's file for a period of seven years, unless the consumer requests that it be removed during that period.[48] During the first five years of this period, the consumer reporting agency is prohibited from including the consumer on any list of consumers provided to a third party offering credit or insurance

to the consumer as part of a transaction not initiated by the consumer.[49] Again, the consumer reporting agency is required to convey the existence of the extended fraud alert to the other consumer reporting agencies, and the consumer is entitled to obtain copies of the consumer's credit report free of charge.[50] Consumers are entitled to two free copies of their credit reports each year if they have placed a fraud alert on their accounts during the preceding 12-month period.[51]

Under FACTA, identity theft victims are entitled to obtain from businesses a copy of the application or other business transaction records relating to their identity theft free of charge.[52] Businesses must provide these records within 30 days of receiving a consumer request.[53] The business may, prior to providing the records, require proof of the consumer's identity and a police report and completed affidavit establishing the identity theft.[54] A business may refuse to provide records if it determines in good faith that the FCRA does not require disclosure, or it does not have a high degree of confidence in knowing the requestor is actually the named consumer.[55]

One of the more significant changes under FACTA is that for the first time, consumers are permitted to dispute the accuracy of information directly with furnishers.[56] They may file identity theft claims with furnishers to prevent them from reporting the information.[57] This right appears at present, however, to be largely illusory because these provisions are not enforceable by a private cause of action.[58]

IV. Protecting Clients from Identity Theft

Like other businesses and professionals who have access to or maintain personal information of customers and clients, attorneys must be cognizant of the need to protect this information. Some of the steps attorneys can take to protect client information include:

- collecting client personal information only where it is necessary to the retention,
- restricting access to client personal information to those who need it,
- storing client files in a secure area where outside vendors and others do not have access,
- never leaving client information sitting on desks overnight,
- never disclosing client information to others unless authorized by law and absolutely necessary,
- wherever possible, avoiding disclosure of client information in public filings; if financial information must be disclosed (i.e. divorce decrees), provide the least amount of information necessary to effect the legal end,
- shredding drafts of instruments containing client personal information that do not need to be maintained,
- protecting and regularly changing computer passwords, and
- shredding all documents to be discarded that contain client personal information.

V. Counseling Identity Theft Victims

Regardless of the precautions taken by attorneys and consumers, identity theft will continue to occur for the foreseeable future. There are a number of steps that identity theft victims should take immediately in order to protect themselves and minimize potential losses.

(1) The identity theft victim should file a report with the local police or police in the location where the identity theft occurred immediately upon becoming aware of the theft. The victim should then obtain the police report number or a copy of the police report (as it will be required to obtain the Security Freeze and Extended Fraud Alert, and some companies may require it to process a notice of identity theft).

(2) The victim should obtain and complete a copy of the Federal Trade Commission Identity Theft Affidavit.[59] The Affidavit is accepted by the three major credit bureaus, participating credit issuers, and most major financial institutions.

(3) The victim should contact the fraud departments of all three major credit bureaus.[60] The victim should have a fraud alert placed on the account and direct that no new credit be extended without personal telephone approval. The credit bureaus should automatically send a copy of the credit report, but the victim should still request one. If there is only a suspicion of identity theft, the victim should request a temporary alert. If the identity theft is certain, the victim should request an extended alert. In either event, the victim should specifically request that a Texas Security Freeze be placed on the credit account.[61]

(4) If another person is arrested and falsely uses the victim's name or personal information, this information may be expunged by contacting the Texas Department of Public Safety.[62]

(5) For any accounts that have been fraudulently accessed or opened, the victim should:

- contact the security department of the appropriate creditor or institution;
- close the account (and perhaps all accounts);
- if necessary, open new accounts;
- use passwords to access those accounts (not a maiden name or SSN);
- where appropriate, request that they cease reporting the information.

(6) The victim should file a complaint with the Federal Trade Commission, which maintains a database of identity theft cases used by law enforcement agencies.[63]

VI. Conclusion

Identity theft is likely to remain a profitable criminal enterprise for some time. By utilizing new procedures available under Texas and federal law, however, consumers will be better able to minimize the effects of identity theft on their credit ratings, limit their financial losses, and reduce the amount of time they spend dealing with these problems.

* J.D., University of Minnesota Law School. Chad Baruch is an attorney in Rowlett, Texas, and is Assistant Principal of Yavneh Academy of Dallas, an Orthodox Jewish college preparatory high school. He is the Treasurer of the Consumer Law Section of the State Bar of Texas.

1. Daren Fonda, *Runaway ID Theft*, TIME, Aug. 4, 2003, at 72. For an excellent discussion of identity theft, *see* George May, *Stop Thief: Are Credit Bureaus and Creditors "Silent" Co-conspirators to Identity Theft*, 5 J. TEXAS CONSUMER LAW 72 (2002).

2. *New Law to Help Combat Identity Theft*, at http://www.consumersunion.org/pub/core_financial_Serv.s/000144.html (last visited January 31, 2005)
3. Federal Trade Commission: ID Theft: *available at* http://www.consumer.gov/idtheft/understanding_idt.html#1 (last reviewed January 30, 2005).
4. *Id.*
5. *Id.*
6. *Id.* (defining pretext calling as the method of getting your personal information under false pretenses).
7. One of the fastest-growing and most successful methods of identity theft is the fraudulent claim letter. The victim, often a single elderly person, receives a foreign letter concerning a sweepstakes victory, inheritance, or need to convey funds to the United States. Those who respond are eventually persuaded to provide their bank account information. The result, predictably, is that the account is emptied. Attorneys need to be aware in advance that it can be very difficult to persuade victims that these letters are fraudulent. Victims want desperately to believe the letters are true – some attorneys and private investigators now collect these letters, in order to be able to show clients the various forms to persuade them the letters are in fact fraudulent.
8. Criminals are creating forgeries of legitimate e-mails and web sites and then stealing personal information with them. Among the most common phishing techniques are through fraudulent web sites for Citibank, U.S. Bank, E-Bay, PayPal, and AOL.
9. Jennifer Barrett, *It's Just Too Easy*, NEWSWEEK, Nov. 2002.
10. *Texas Tech Bill Briefs – 2003 78th Regular Session*, (SB473), available at http://www.depts.ttu.edu/ogr/Legislative%20Report%20-%2078th%20Legislature,%20Regular%20Session.htm (last visited January 31, 2005); TEX. BUS. & COMM. CODE § 23.031 (Vernon Supp. 2004).
11. Credit Report Security Alert, *available at* http://101-identitytheft.com/alert.htm (last visited January 30, 2005).
12. TEX. BUS. & COMM. CODE §§ 20.01(7), 20.031. [Preempted by H.R. 2622, § 202, adding FCRA § 605(i), 15 U.S.C. § 1681c(i).]
13. Richard M. Alderman, *Security Freeze*, at http://www.law.uh.edu/peopleslawyer/SecurityFreeze.html (last visited January 31, 2005).
14. *Id.*
15. *Id.*
16. *Id.*
17. *Id.*
18. *Security Freeze* at n. 13 *supra*.
19. TEX. BUS. & COM. CODE § 20.034 (Vernon Supp. 2004).
20. TEX. BUS. & COM. CODE § 20.034(a) (Vernon Supp. 2004); Brian Bergstein, *Freeze Can Help Against ID Theft*, Associated Press, *available at* http://www.sjpc.org/idtheft/freeze.htm (last reviewed January 30, 2005).
21. TEX. BUS. & COM. CODE § 20.034 (a), (b) (Vernon Supp. 2004).
22. *Id.*
23. *Id.*
24. TEX. BUS. & COM. CODE § 20.034 (c) (Vernon Supp. 2004).
25. TEX. BUS. & COM. CODE § 20.034 (d) (Vernon Supp. 2004).
26. The original amount of the fee was limited to $8, with annual increases authorized proportionally based upon the Consumer Price Index. TEX. BUS. & COMM. CODE §20.04 (Vernon Supp. 2004).
27. TEX. BUS. & COM. CODE § 20.035 (Vernon Supp. 2004).
28. TEX. BUS. & COM. CODE § 20.036 (Vernon Supp. 2004).
29. *Id.*
30. *Id.*
31. TEX. BUS. & COM. CODE § 20.037 (Vernon Supp. 2004).
32. TEX. BUS. & COM. CODE § 20.038 (Vernon Supp. 2004).
33. TEX. BUS. & COM. CODE § 20.039 (Vernon Supp. 2004).
34. TEX. BUS. & COM. CODE § 20.12 (Vernon Supp. 2004).
35. 15 U.S.C. § 1681 et seq. (2003).
36. Pub. L. 108-159, 111 Stat. 1952.
37. *Fact Sheet 6(a): Facts on FACTA*, 1. Introduction, at http://www.privacyrights.org/fs/fs6a-facta.htm (last visited January 31, 2005).
38. *Id.*
39. Facts on FACTA, *available at* http://www.privacyrights.org/fs/fs6a-facta.htm (last reviewed January 30, 2005).
40. *Id.*
41. *Id.*
42. *Id.*; The Fair Credit Reporting Act as Amended Jan 2004, 2B. Fraud Alerts and Active Duty Alerts *available at* http://www.creditinfocenter.com/legal/FCRA.shtml (last reviewed January 30, 2005).
43. *Id.*
44. 15 U.S.C. § 1681 (Supp. 2004).
45. 15 U.S.C. § 1681c-1(a) (Supp. 2004).
46. *Fact Sheet 6(a): Facts on FACTA*, 2B. Fraud Alerts and Active Duty Alerts, *available at* http://www.privacyrights.org/fs/fs6a-facta.htm (last visited January 31, 2005).
47. Consumer Union Org., *available at* http://www.consumersunion.org/creditmatters/creditmattersfactsheets/001626.html (last reviewed January 30, 2005).
48. 15 U.S.C. § 1681c-1(b) (Supp. 2004).
49. *Id.*
50. *Id.*
51. *Id.*; Consumers Union.Org, *available at http://www.consumersunion.org/creditmatters/creditmattersfactsheets/001626.html*, (last reviewed January 30, 2005).
52. 15 U.S.C. § 1681g(e)(1).
53. *Id.* Privacy Rights Clearinghouse, *available at* http://www.privacyrights.org/fs/fs6a-facta.htm, (last reviewed January 30, 2005).
54. 15 U.S.C. § 1681g(e)(2).
55. *Id.*
56. 15 U.S.C. § 1681s-2(a)(8).
57. 15 U.S.C. § 1681s-2(a)(1).
58. 15 U.S.C. § 1681s-2(d).
59. The affidavit can be found at www.consumer.gov/idtheft/affidavit.pdf.
60. Equifax, P.O. Box 740241 Atlanta, GA., 30374-0241, (800) 525-6285, www.equifax.com; Experian, P.O. Box 2104 Allen, Tx., 75013, (888)387-3742, www.experian.com; TransUnion, Fraud Victim Assistance Division, P.O. Box 6790 Fullerton, Ca., 92634, (800)680-7289, www.tuc.com.
61. To obtain a Texas Security Freeze, the request must be made by Certified Mail, include a copy of the police report, and provide proper identification.
62. TDPS phone number: 512-424-5258.
63. Federal Trade Commission, Identity Theft Clearinghouse, Federal Trade Division, 600 Pennsylvania Avenue, NW, Washington, D.C., 20580, www.consumergov.idtheft, (877)438-4338.