INSTITUTE OF CONSUMER FINANCIAL EDUCATION

IDENTITY THEFT RISK MANAGEMENT SURVEY AND REPORT

SUMMARY FOR HOLDERS OF PROTECTED INFORMATION GUIDE

August 2008

Based on an extensive proprietary survey of providers of Identity Theft risk management services, and additional related research, this Report by ICFE provides a basis for entities that hold protected confidential consumer information to make informed decisions on using such services.

It is important to understand the risk of people whose information is compromised becoming a victim of identity theft, so a good choice can be made. There are generally three types of programs that meet various needs:

- Broad-based monitoring and notification services
- Credit-report monitoring and "freeze" or "fraud alert" programs
- Restoration and Specialty programs (such as medical, employment, or criminal data)

Typically, the decision to select a provider of identity theft risk management services occurs when the organization responsible for maintaining the confidentiality of protected consumer information has experienced a breach and must take action to prevent or minimize the damage to potential identity theft victims whose personally identifiable information has been inadvertently captured by or released to unauthorized parties.

Many of the considerations for selecting such a service are similar to those for the individual consumer in managing this risk. Of special importance is an assessment of the nature of the risk, based on the type of information that has been compromised and any available knowledge about the unauthorized party in possession of the information.

In this context, it is critical to realize that the expectation of the person whose information has been breached is not the determining factor about what choice should be made. If the breached information would give rise to the creation of false identity

documents or perpetrating employment fraud, for instance, little effect would be accomplished by concentrating solely on prevention of new account fraud.

Of special interest in this regard is the national Identity Theft Standards Panel initiative [•]

First, the breached entity, whether it be a business, public or government agency, non-profit organization, or other holder of protected information, must evaluate the nature of the information that has been breached and vulnerabilities of the individuals whose information has been compromised.

In general, there are two categories of such information:

- Financial information, such as the specifics that are present in credit reports.

- Non-Financial information, of the type that does not appear in credit reports, such as employment histories, salary specifics, drivers licenses, criminal records, medical information such as health histories and drug-related items, and would typically be information on employees and receivers of benefits.

Once the determination is made as to type of information and the kinds of vulnerability to which the individuals might be subjected, the decision on the appropriate risk management and damage control program to employ can be made.

Common provisions of such programs are similar to those offered to consumers; for this purpose, it is appropriate to incorporate by reference the Tables in the Consumer Section above.

Two important distinctions should be observed, based on needs of the parties:

- Consumers making a choice among the various risk management providers start from the assumption that their identities have not been compromised, and they have an open choice as to which features best fit their needs.

- Holders of protected information who have suffered a breach of confidentiality need to control various types of potential damage that can result from the breach; beyond the damage to the affected individuals, the damage to the enterprise can include loss of public confidence, loss of

[•] The Identity Theft Prevention and ID Management Standards Panel (IDSP) organized by the American National Standards Institute (ANSI) and the national Better Business Bureau (BBB) continues to work toward the identification and adoption of standards for remediation in the event of a breach of confidentiality of personally identifiable information protected by law and regulation; ICFE has been an active participant in this process, and has advocated for the adoption of a standard under which the remediation steps closely reflect the nature and vulnerability of the breached information.

customer base, damage to employee loyalty and retention, and other adverse consequences to the organization.

One recent phenomenon that should be put into perspective is the claim that consumers will be satisfied if their expectations are met in response to a breach of their protected information. Unfortunately, the expectations of the consumer are often based on either unrealistically high standards or unreasonably low standards under which the actual vulnerability of the breached information is simply not taken into account.

It does not help to give the consumer a false sense of security that no harm can befall him or her from the breach of personal information, in circumstances where the prevention program does not have the required depth or breadth.

The most direct example would be the case in which the compromised information is of the Non-Financial variety mentioned above. Securing the credit files to prevent the opening of new accounts in the victim's name does nothing to protect against misuse of personal information to commit employment fraud, medical and benefit abuse, get a drivers license, or engage in criminal activity to the detriment of the victim.

ICFE's experience as well as information collected in the course of the Survey indicate that the per-person costs of obtaining identity theft risk management coverage for the benefit of those whose information is compromised are variable and subject to negotiation. It is notable that there are pricing break-points that can be applied to calculate upfront costs for a given number of individuals to have access to the program, and lesser per-activation charges payable at the time an individual actually enrolls.

<u>Broad-based monitoring and notification</u>

Based on the ICFE's extensive research, the most effective means of preventing identity theft, and minimizing damage to the victim, is with a broad-based monitoring and notification service. These are the essential elements of such a service:

- Depth and breadth of data bases monitored
- Immediate notification to the consumer of any anomalies
- Individualized risk assessment feature
- Means of predicting and stopping the misuse of personally identifiable information
- Restoration components can complete the safety net of coverage.

The Respondents in this category are:

- IdentityTruth
- IDSafeguards/IDExperts*
- Intersections/IdentityGuard
- ITRisk Managers
- SecureIDSystems/FNB Merchants

Broad-Based Providers	Identity Truth	ID Safeguards/ID Experts**	Intersections/ Identity Guard	ITRiskManagers	SecureIDSystems/ FNBMerchants
Data Bases Monitored	Breach information, Internet sites trading SSN, credit and personal data, and utility accounts	Real property records, criminal records, land & cellular phone records and vehicle ownership records	Public Records/Criminal	No	Utilities, dmv records, SSA, telco
Immediate Notification	Yes	Monthly	Yes	No	Yes
Risk Assessment	Yes	No	Yes	Self-Assess	Yes
Predictive Technology	Yes*	No	Activity Calculator	No	Pattern Changes
Restoration	Yes (RelyData)	Yes	Recovery Unit***	Yes****	Managed*****
Guarantee/Insurance	Both	Insurance	Insurance	Insurance	Insurance
Price	70-120/year Individual	Individual 139.95/year Family 269.95/year	60-216/year 39.95 One-Time add-on Many Addtl. Options	12-160/year	Individual 84/year Family 156/year
	*Proprietary technology allows prediction of possible identity fraud	**Formerly IDSafeguards, withdrew 3rd-party restoration service for LifeLock	***At 14.99/month	****2 Levels of Consumer Input Moderate Range	*****Substantial Consumer Input
Average Price for All Providers in All Categories is approximately $108 per year					

Credit-report monitoring and "freeze" programs

It is a common misconception that all incidents of identity theft are financial in nature, and can be prevented or avoided by taking actions on consumer credit files. In fact, official statistics indicate that one-third to one-half of all cases reported to the Federal Trade Commission (FTC) are of types that do not appear in credit reports.

Nonetheless, consumer-oriented identity theft risk management programs that couple credit report-related actions with restoration services can be effective, though not necessarily fully preventive.

In order to accomplish their risk management mission, the essential features of these programs include:

- Continuous monitoring of credit reports, preferably in all three of the major credit reporting agencies
- Prompt notification to the covered party in the event of any reportable event
- Capability to impose a credit freeze or fraud alert on behalf of the covered party, upon determination that such an action is appropriate and effective
- Pro-active search of other data bases in the event that a covered party becomes a victim of identity theft
- Restoration/recovery service for identity theft incidents that are outside the purview of the credit report, such as employment, benefit, medical, drivers licenses, or criminal activities committed using the identifying information of the covered party

The Respondents in this category are:

- Equifax
- Experian
- IdentityForce
- Kroll *
- LifeLock **
- TransUnion

Credit-Report Based Providers

	Equifax	Experian	IdentityForce	Kroll	LifeLock	TransUnion
Data Bases Monitored	1 or 3 CRAs	1 or 3 CRAs	Public Records/Criminal	1 or 3 CRAs	No	1 or 3 CRAs
Immediate Notification	Yes	Yes	Yes	Yes	Yes	Yes
Risk Assessment	No	No	No	Self-Assess	Yes****	No
Freeze or Fraud Alert	By Request	By Request	By Request	By Request	Freeze	By Request
Restoration	Yes*	Yes**	Yes***	Yes***	Yes****	Yes*****
Guarantee/Insurance	Insurance	Insurance	Insurance	Insurance	1MM Guarantee	Insurance
Price	70-170/year	60-360/year	Basic 39.95/year Complete 139.95/year	156/year Numerous Configurations	Individual 110/year Child 25/year	180/year
	*Substantial Consumer Input	*Provided by RelyData	***Licensed Investigators	***Licensed Investigators	****No Staff Details, requires Substantial Consumer Input	*****Provided by TransUnion LLC

Average Price for All Providers in All Categories is approximately $108 per year

* Kroll also provides post-incident searches of other data bases and restoration services.

** As of the date of the survey, this provider said they would expand to other databases, but as of the date of this Report, it does not appear to be in place; restoration services were formerly provided by IDSafeguards/IDExperts, but are now apparently in-house.

Restoration and Specialty programs

Providers that do not fit neatly into either of the above two categories are assigned to this specialty group. They include providers of proprietary programs, private label services, and restoration specialists. Key features of their services include:

- Information and monitoring of specialized data bases, such as medical and criminal
- Restoration services only, based on insurance-premium type pricing scale
- Establishment of a Personal Identity Profile and monitoring of the elements of such individual profiles
- Direct expense reimbursement as an alternative to insurance
- Self-monitoring of selected data bases, and proprietary systems for self-help by consumers

The Respondents in this category are:

- Fraud Prevention Institute
- ID Armor
- Intelius/ID Watch
- RelyData
- Truston

NOTE: To varying degrees, providers in other categories offer restoration services: ITRisk Managers, IDSafeguards/IDExperts, and Kroll

Table 3 - Specialized Providers	Fraud Prevention Institute	ID Armor	Intelius/ID Watch	RelyData	Truston
Data Bases Monitored	Medical, Criminal	None	Proprietary Profile	All 3	Chex Systems Member Monitors Others
Immediate Notification	1 week	N/A	Yes	Yes	N/A
Risk Assessment	Yes	No	Profile Process	Yes - Actual Events	No
Freeze or Fraud Alert	N/A	N/A	N/A	By Request Only	No
Restoration	Yes	Yes*	No	Yes**	"Prescriptive Workflow"***
Guarantee/Insurance	No	No	Insurance	Expense Reimbursement	No
Price	Free	23.88/year	60-120/year based. on Term	Private Contract	Free-$120/year
		* Minimal effort for Client		** Minimal effort for Client **Private Label for Numerous Providers & Organizations	***Substantial Consumer Input
	***Also See Entries for Providers in Other Categories for Restoration Services: ITRisk Managers, IDSafeguards/IDExperts, & Kroll				
	Average Price for All Providers in All Categories is approximately $108 per year				

COMMENTS ON GUARANTEES AND INSURANCE

Guarantees

Several of the providers "guarantee" the effectiveness of their services in preventing identity theft. Like all guarantees, the value is no greater than the terms and conditions – and especially the limitations. In most cases, the "guarantee" provides for restoration services, but only if the incident of identity theft is a result of the failure of the underlying prevention program. The most valuable of such guarantees are those in which the restoration services are carried out by specialized third party providers or in-house licensed investigators.

Insurance

Several of the providers include an insurance component in their programs. The insurance feature typically covers reimbursement for out-of-pocket expenses incurred to restore the integrity of the victim's identity; most include a "lost work time" provision with a cap of $500 per week for 4 weeks. There are numerous limitations and conditions on the coverage. Deductibles range from zero to $250, with a common maximum coverage amount of $25,000.

Similar coverage is offered by many insurance companies as a rider to homeowners or renters insurance, at a nominal additional premium or even at no additional cost.

In general, ICFE believes that the inclusion of an insurance feature in an identity theft risk management programs is not a sufficient consideration to make it a better choice than a program without insurance.

ADDITIONAL CONSIDERATIONS FOR CONSUMERS IN MAKING DECISIONS

- Early discovery and notification of all types of identity theft-related incidents are paramount; most damage is done between time of the breach and the victim becoming aware of the problem

- Prompt action is required to minimize damages and to recover the integrity of the elements of the victim's identity

- Willingness to participate actively in the recovery and restoration process is an important consideration

- Make informed choices on the elements that are most important to the individual consumer -- and then act on them.

ABOUT THE INSTITUTE OF CONSUMER FINANCIAL EDUCATION

The ICFE www.icfe.info was founded in 1982 by the late Loren Dunton (creator of the "certified financial planner" (CFP) designation) and it is dedicated to helping consumers of all ages to improve their spending, increase their savings accumulation and use credit more wisely. The ICFE trains and certifies Personal Finance Instructors for its own curriculum, "The Money Instruction Book." It also professionally trains Certified Credit Report Reviewers and Certified Identity Theft Prevention Risk Management Specialists.

The ICFE is an award winning, nonprofit, public education organization that has helped millions of people through its education programs and resources. It publishes the Do-It-Yourself Credit File correction Guide which is now in its 22nd printing. The ICFE has distributed over one million "Credit/Debit Card Warning Labels" and "Credit/Debit Card Sleeves" world wide.

The ICFE became an official partner with the Department of Defense/Financial Readiness Campaign in June of 2004. Since 2005, ICFE has certified over 5,000 individuals as CCRR, CITRMS and Instructor qualified professionals who are employed by a wide range of organizations including financial institutions; mortgage, real estate, and financial services firms; corporations; law enforcement, US military and other government agencies. Many others are privacy and security practitioners and consultants.

The Institute of Consumer Financial Education 2008 Identity Theft Risk Management Survey and Report initiative was headed by Yan Ross, CITRMS®, ICFE's Project Manager for the Certified Identity Theft Risk Management Specialist Program. Special thanks go to Evan Whalley, CITRMS®, of Desert Solutions, LLC, for his participation in this initiative.

ABOUT THE SPONSOR

IdentityTruth is the leading provider of a new breed of service to help consumers safeguard their Privacy and Identity. Through innovative technology, individuals receive the earliest possible notification™ in advance of potential misuses of their identities so they can take better control. Early detection is the best protection. IdentityTruth is a privately held, VC- funded company headquartered in Waltham, Massachusetts.