Working Together to Prevent Identity Theft

Consultation Workbook

Request for Comments

The Consumer Measures Committee (CMC) is a forum of federal, provincial and territorial government representatives who cooperate to eliminate barriers to trade between provinces and territories, and to improve the marketplace for Canadian consumers. The CMC is conducting a public consultation on measures to address Identity Theft with the objective of soliciting views from stakeholders and the public on their policy and practical implications. The CMC will then revise and refine the proposals based on stakeholder feedback. A subsequent round of consultations will be held on specific proposals presented in quasi-legislative language, with an indication of which statute(s) would be affected.

By providing background on the issues and a preliminary analysis of the various options for reform, the Discussion Paper ***Working Together to Prevent Identity Theft*** is intended to facilitate public participation in the reform process.

In order to assist the CMC in reviewing submissions, please structure your comments on the same basis as the Discussion Paper, or use this Workbook. In particular, please provide responses to individual questions, as well as any additional comments you may have. Please focus on developments that can reasonably be expected to occur over the next 10 years and provide as much detail and supporting evidence as possible.

We ask all parties to do their best to assist the CMC in achieving its challenging goal of developing recommendations for the best framework for combating identity theft - irrespective of the short-term costs and benefits for various industry players or consumer groups.

We would greatly appreciate if you would submit your comments electronically by **September 15th, 2005**. To do so, please enter your responses and e-mail this workbook to us, at:

E-mail: info@cmcweb.ca

If you prefer to provide a hard copy of your submission, please send it, along with your name and contact information to:

Mail: Consumer Measures Committee
c/o Office of Consumer Affairs
Industry Canada
235 Queen Street,
Ottawa (ON) K1A 0H5

If you wish to submit comments on the *Discussion paper* and options, it is not essential that you use the *Consultation workbook*. You may choose to provide comments in letter form or in an e-mail and if you

prefer, to limit your comments to just a few of the options outlined.

All materials or comments received from organizations may be used and disclosed by the Consumer Measures Committee (CMC) or any government body to assist in evaluating and revising the proposed options described below. This may involve disclosing materials, comments or summaries of them, to other interested parties during and after the public comment period.

An individual who provides materials or comments and who indicates an affiliation with an organization will be considered to have submitted those comments or materials on behalf of the organization so identified.

Materials or comments received from individuals who do not indicate an affiliation with an organization may be used and disclosed to assist CMC or other government bodies in evaluating and revising the proposed options. However, CMC or other government bodies will not disclose personal information, such as an individual's name and contact details, unless required by law.

NOTE: As you type your response, the space below the question will expand to enable you to put as much text as you wish.

Your Contact Information

First Name: Chris

Last Name: Hoofnagle

Organization & Address:

Electronic Privacy Information Center, West Coast Office
944 Market St. #709, San Francisco, CA 94102
415-981-6400
Hoofnagle@epic.org

First, let us express our appreciation for your efforts in working to address identity theft. The US government has taken a reactive approach to the crime, and our law addresses the crime by creating remedial measures and heightened penalties. These remedial measures (such as the "fraud alert") help consumers but do not prevent the crime. Similarly, heightened criminal penalties have been ineffective as well, because impostors are so rarely caught. We applaud your proactive approach to this difficult problem.

Since the Committee is seeking solutions over the next ten years, we urge the consideration of bold approaches to address identity theft. We are still in a world where credit cards are being used as the principal form of electronic payment. This is a system where the exact same number is being used over and over to charge accounts, without a PIN or other method of effective authentication. This number is given to hundreds of people—cashiers, waiters, payment processors, and unknown web merchants—creating an incredible array of individuals who could use the number for fraud. Without pressure from consumer protection authorities, there is little evidence that this broken system will be fixed.

Although unaddressed by the Committee, one bold approach would be the pursuit of methods of payment that promote anonymity, thereby heightening privacy and reducing the risk that identity can play a role in committing fraud.

Please feel free to call upon us for further comment or assistance.

We begin our comment by providing feedback on the four sections of the paper.

Section 1: Definition of Identity Theft

The existing definition of identity theft unnecessarily limits identity theft to the unauthorized use of personal information to commit a crime. Under the current definition, it is not clear that identity cloning, i.e. adopting another individual's identity would be considered identity theft. The use of an individual's personal information, even without the subsequent commission of a crime, can be incredibly problematic for the consumer. Consumers can suffer incredible mental anguish and hassle from the knowledge that their personal information has been inappropriately acquired. Consequently, the commentators believe the definition of identity theft should drop the requirement "to commit a crime, such as fraud, theft, or forgery."[1] The revised definition is consistent with that adopted by the UK Home Office Identity Theft Steering Committee.

Section 2: Understanding the Problem

The discussion paper identifies certain consumer behaviour, such as failure to protect the PIN, providing more information than necessary, and use of insecure web sites as culprits for exacerbating identity theft. We believe that these factors are not major causes of identity theft. They should not distract the Committee from the realities of identity theft, which include the fact that the crime is so easy to commit that even individuals under the duress of methamphetamine addiction can organize criminal identity theft syndicates.

We also urge the Committee to not be distracted by claims that the identity theft problem lies with sophisticated hackers from other nations. While these actors do contribute to the overall identity theft problem, the principal causes of identity theft are business practices that make it extremely easy to commit the crime, and the reliance upon the Social Security number.

[1] The UK Home Office Identity Theft Steering Committee explains "identity theft occurs when your personal information is used by someone else without your knowledge." http://www.identity-theft.org.uk/ accessed on September 2, 2005.

In *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*,[2] EPIC's Chris Hoofnagle identifies several economic forces that drive identity theft: First, under the Fair Credit Reporting Act (FCRA), credit reporting agencies only are required to "maintain reasonable procedures designed" to prevent unauthorized release of consumer information.[3] The Federal Trade Commission Commentary on the FCRA specifies that this standard can be met in some circumstances with a blanket certification from credit issuers that they will use reports legally.[4] This certification standard is too weak. It allows a vast network of companies to gain access to credit reports with little oversight. It treats credit issuers and other users of credit reports as trusted insiders, and their use of credit reports and ultimate extension of credit as legitimate. A trust network of that size requires significant auditing and training, and blanket certifications cannot guarantee adequate oversight over such a large number of people with access to the credit network.

Second, credit grantors do not have adequate standards for verifying the true identity of credit applicants. Credit issuers sometimes open "tradelines" (a new account) to individuals who leave obvious errors on the application, such as incorrect dates of birth or fudged Social Security Numbers. For instance, in *Nelski v. Pelland*, 2004 U.S. App. LEXIS 663 (6th Cir. 2004), a phone company issued credit to impostor using the victim's name but slightly different Social Security Number). In *United States v. Peyton*, 353 F.3d 1080 (9th Cir. 2003), impostors obtained six American Express cards using the correct name and Social Security Number of employees-victims but directed all six to be sent to the impostors' home. In *Aylward v. Fleet Bank*, 122 F.3d 616 (8th Cir. 1997), the bank issued two credit cards based on matching name and Social Security Number but incorrect address. In *Vazquez-Garcia v. Trans Union De P.R.*, Inc., 222 F. Supp. 2d 150 (D.P.R. 2002), an impostor successfully obtained credit with matching Social Security Number but incorrect date of birth and address. In *Dimezza v. First USA Bank, Inc*., 103 F. Supp. 2d 1296 (D.N.M. 2000), an impostor obtained credit with a Social Security Number match but incorrect address. In light of these cases where individuals fudged the application and still obtained credit, identity theft expert Beth Givens has argued that many incidences of the crime could be prevented by simply requiring grantors to more carefully review credit applications for obviously incorrect personal information.[5]

Third, competition to obtain new customers drives creditors to grant new accounts without proper authentication. Grantors have flooded the market with "pre-screened" credit offers, pre-approved solicitations of credit made to individuals who meet certain criteria. These offers are sent in the mail, giving thieves the opportunity to intercept them and accept credit in the victim's name.[6] Once credit is granted, the thief changes the address on the account in order to obtain the physical card and to prevent the victim from learning of the fraud.[7] The industry sends out billions of these pre-screened offers a year. It 1998, it was reported that 3.4 billion were sent.[8] In 2003, the number increased to an estimated 5 billion.[9]

---

[2] SECURING PRIVACY IN THE INTERNET AGE, Stanford University Press, 2005, available at http://ssrn.com/abstract=650162.

[3] 15 U.S.C. § 1681e(a).

[4] The Federal Trade Commission is statutorily barred from promulgating regulations on the FCRA. 15 U.S.C. § 1681s(a)(4). The agency issues a non-binding commentary on the Act. Credit, Trade Practices, 16 CFR § 600, 607 (1995).

[5] *Legislative Hearing on H.R. 2622, The Fair and Accurate Credit Transactions Act of 2003, Before the Committee on Financial Services*, Jul. 9, 2003 (testimony of Chris Jay Hoofnagle, Deputy Counsel, Electronic Privacy Information Center).

[6] *Identity crises -- millions of Americans paying price*, CHI. TRIBUNE, Sept. 11, 2003, p2.

[7] *Id*.

[8] *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, Hearing Before the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information*, Jul. 12, 2000 (testimony of Beth Givens, Director, Privacy Rights Clearinghouse) (*citing* Edmund Sanders, *Charges are flying over credit card pitches*, L.A. TIMES, Jun. 15, 1999, p. D-1), available at http://www.privacyrights.org/ar/id_theft.htm.

[9] Rob Reuteman, *Statistics Sum Up Our Past, Augur Our Future*, ROCKY MOUNTAIN NEWS, Sept. 27, 2003, p 2C; Robert O'Harrow, *Identity Crisis; Meet Michael Berry: political activist, cancer survivor, creditor's dream. Meet Michael Berry: scam artist, killer, the real Michael Berry's worst nightmare*, WASH. POST MAG., Aug. 10, 2003, p W14.

In 2005, Direct Magazine reported, "Credit card marketers sent out a record 1.4 billion direct mail offers during the first quarter, up 11% over last year, according to Synovate…With the record high mail volumes, the response rates to credit card offers reached a record low of 0.4 percent."[10] One professor who kept all of his junk mail after moving for a new job received 69 credit offers in 10 months.[11] 20 of the 69 offers were from a single issuer—Capital One.

As part of our recommendations, we urge the Committee to give individuals greater control over the sending of these pre-screened offers of credit. Companies should send these offers on an opt-in basis, because on an opt-out basis (as they are sent in the US), they are regularly intercepted by criminals who need little sophistication to use them for identity theft.

The white paper notes that "certain corporate practices….encourage what the police call 'dumpster diving…'" These fraud practices could be limited by adopting regulations that place the responsibility on data users to destroy documents that contain sensitive personal information securely. In the U.S., the Fair Credit Reporting Act requires all users of credit reports to securely dispose of information by shredding or by "electronic shredding," where the information is stored on a computer.[12]

The discussion draft notes that credit card companies bear the burden of much of the cost of identity theft. The draft neglects to mention the cost to merchants—an enormous portion of the cost of identity theft is absorbed by merchants who accept charges from cards issued to impostors through the "chargeback" system. Cost is also carried by consumers, who spend hundreds of hours attempting to straighten their financial history. In any calculus of the cost of identity theft, the time spent by individuals rectifying their good name should be included.

Part 3: Legislative landscape:

The commentators question the decision to benchmark to the United States legislation given that "identity theft is a much larger problem in the US than it is in Europe or Australia." US federal legislation has not attempted to *prevent* identity theft in a meaningful way. Instead, the trend in the US is to give consumers remedial rights, and to heighten criminal penalties against impostors. It is only in recent years that states within the country have passed preventative measures in form of "credit freeze," which we will comment upon *infra*. Credit industry lobbyists have attempted to "preempt" or supersede these laws with weak federal frameworks that give consumers little or no rights.

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) did little to prevent identity theft; however, it did establish remedial mechanisms for victims once the crime had been committed. Already consumers have experienced difficulty with these new remedial measures. FACTA's 90-day fraud alert, for instance, is too short to protect consumers. The longer, 7-year fraud alert is difficult to establish because it requires a police report, but some police departments will not issue a report in identity theft cases. Finally, one provision of FACTA allows victims to obtain business records from companies that established fraudulent accounts in their names. Victims report that companies are not releasing these records, and that they are requiring a subpoena for victims to exercise the right.

[10] *CC Marketers Send Out 1.4 Billion Offers, Response Dips*, Jul. 15, 2005, available at http://directmag.com/news/cc-071805/

[11] Bob Sullivan, *Deluged with credit card mail? Help is coming*, MSNBC, Aug. 8, 2005, available at http://msnbc.msn.com/id/8827007/.

[12] Disposal of credit report information and records, 16 CFR 682 (2005), available at http://www.access.gpo.gov/nara/cfr/waisidx_05/16cfr682_05.html.

Option I – Truncate (partially blank out) payment card numbers

Persons that accept payment cards (including credit cards and debit cards) for the transaction of business must not print the expiry date or more than the last five digits of the card number on any receipt generated electronically at the point of sale or transaction.

1. Do you think this option would better protect against identity theft?

Yes

Why or Why not?

The credit card industry designed the payment network in such a way that consumers use a single number over and over, combined with a poorly-implemented form of authentication (signature verification) to make charges. Any policy that reduces the ease with which individuals can obtain the credit card number should reduce fraud.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

No comment.

3. Should there be exemptions? If yes, what type?

Any exemptions should apply only to small businesses that face compliance challenges. Exemptions should be time limited.

4. Should there be a penalty associated with this provision (as proposed in Option 9)?

Yes, there should be penalties associated with this provision to encourage compliance.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

Consumers should not be held responsible for the design decisions of the credit card industry. The industry has prioritized quick payment over security, and has refused to implement better authentication measures (such as a PIN) that could reduce credit card fraud.

Credit card companies and merchants should bear the costs associated with the security weaknesses inherent in the payment system they designed.

6. Are there disadvantages for consumers or industry? Please describe.

No comment.

7. What are the existing or planned industry standards for truncation of payment cards, and if any, what are timelines for implementation? Do the standards exclude handwritten and/or imprinted cards?

No comment

Option II – Verify the identity of persons and organizations accessing credit reports

Credit bureaus must take reasonable steps to authenticate the people and organizations that are accessing credit reports.

1. Do you think this option would better protect against identity theft?

Yes, but it should be strengthened.

Why or Why not?

At a minimum, consumer reporting agencies should use "reasonable steps" to authenticate report users. Consumer reporting agencies are in the best position to verify organizations accessing a credit report. But there are market incentives to shoddy verification (the potential sale of more credit reports), and regulation will be required to ensure that consumer reporting agencies adequately vet their clients.

As noted *supra*, users of credit reports can sign blanket statements claiming that they are in compliance with the FCRA. This is inadequate. There must be real training and auditing in place to determine whether reports are being pulled without a permissible purpose.

Choicepoint, a US-based commercial data broker, recently sold over 100,000 files to a criminal posing as a business in California. As a result, Choicepoint is now performing site visits before establishing new accounts. We think a similar standard should be in place to users of the credit system.

On the other hand, consumer reporting agencies have a market incentive to engage in more strenuous authentication where the consumer is trying to obtain their own report. That is because under US law, individuals are now entitled to a free report from the nationwide consumer reporting agencies. There have been many complaints from consumers that consumer reporting agencies have made it too difficult to request their free reports. Over 1,600 people have lodged complaints with the Federal Trade Commission because they were unable to obtain their free report online.[13]

Obviously, there needs to be adequate authentication to prevent reports from falling into the wrong hands, but it is suspicious that the free report site employs heightened authentication while businesses can pull a report with little oversight.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

Consumer reporting agencies should bear the costs of authenticating the people and organizations that are accessing credit reports.

3. Should there be exemptions? If yes, what type?

No.

4. Should there be a penalty associated with this provision (as proposed in Option 9)?

Yes, there should be a penalty for the unauthorized release of credit reports. The FCRA has criminal and civil penalties for unauthorized access of a report.

---

[13] Caroline E. Mayer, *Order Free Credit Reports, Then Cross Your Fingers*, Sept. 1, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/08/31/AR2005083102575_pf.html.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

Since consumer reporting agencies are the data holders, they should bear the responsibility to protect the data. Consumers cannot opt out of credit reporting, so they should not bear the burden of the system's mistakes.

6. Are there disadvantages for consumers or industry? Please describe.

No comment.

7. Should this obligation to authenticate be required of third party resellers of credit reports? If not, why not?

Yes. All organizations that deal in personal information should have an obligation to authenticate the individual or organization accessing the personal information. Consumers should be aware of each instance that their personal information is released. Without the duty to authenticate, report users will be given an incentive to use third party resellers.

8. Do credit bureaus provide different levels of information in credit reports depending on the need of the organization and/or individual requesting the credit report? If so, what standards are applied?

Consumer reporting agencies do sell "credit headers," identification information from credit reports, to many different companies and individuals. The sale of credit headers was limited by the Gramm-Leach-Bliley Act of 1999, but we think that credit headers should be "moved below the line." That is, a credit header should only be sold to a person who has a permissible purpose to obtain the information, and the header should be treated with the same regulations and procedures for disclosure and destruction as a full credit report.

Consumer reporting agencies also operate massive data marketing businesses. These businesses apparently sell data that does not fall subject to the FCRA (with the possible exception of the credit header). They collect information in a variety of ways (including consumer surveys, collecting information from call centers, and using automated methods such as "Automatic Number Identification," a type of Caller ID transmitted when making a call).

9. What would be the costs associated with authenticating credit lenders and consumers?

Consumer reporting agencies should bear the cost.

Option III – Do not disclose social insurance numbers (SINs) on credit reports or use them as a unique identifier for consumers

Where it is appropriate for financial institutions to collect SINs, they should keep the numbers confidential. In particular, consumer reporting agencies and financial institutions should not use a SIN as a unique identifier for consumers, or disclose the consumer's SIN on a credit report.

1. Do you think this option would better protect against identity theft. Why or why not?

In the US, the Social Security number (SSN) is used both for identification and authentication. Accordingly, the SSN has become the key to identity theft.[14] The CMC should seek to avoid recreating the US situation in Canada. Restrictions on collection and use of the SIN will serve to reduce the risk that the private sector will adopt the SIN as a universal identifier and authenticator.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

This option would reduce the risk of identity theft, thus providing savings to both businesses and consumers.

3. Should there be exemptions? If yes, what type?

Exceptions to collection and use of the SIN should encourage, where possible, transition to an alternative identifier. For instance, where SINs are used in appropriate contexts, the government can establish a time-limited exemption to allow the entity to transition away from the SIN.

4. Should there be a penalty associated with this provision (as proposed in Option 9)?

Yes. In the US, the key to protecting privacy is limiting the disclosure of the SSN. Unfortunately, many different entities have access to the identifier, and some post it on the Internet or otherwise disclose it inappropriately. In order to limit dissemination of the identifier, individuals will need laws to assist them when the SIN is in the database of another.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

Institutions that collect and maintain unique identifiers in their course of business should be responsible for their misuse or disclosure.

6. Are there disadvantages for consumers or industry? Please describe.

The benefit to consumers from a reduction of reliance on the SSN/SIN will be greater privacy. There is less of a risk that profiles can be aggregated on a person if use of unique identifiers is limited. Furthermore, using different identifiers limits the risk of "placing all one's eggs in a single basket." That is, under the current system, there is only one key to identity—the SSN. Using different identifiers for different purposes can soften the blow of a security breach or identity theft.

7. For financial institutions, is there an industry standard with respect to requesting the SIN? If so, when is it requested and when is it not requested. What are the grey areas?

No comment.

---

[14] Letter from Chris Jay Hoofnagle, Associate Director, EPIC and Edmund Mierzwinski, Consumer Program Director, US PIRG, to Representative Clay Shaw, Chairman, House Ways and Means Subcommittee on Social Security, Jul. 2, 2004, available at http://epic.org/privacy/ssn/ssnanswers7.2.04.html.

8. For retailers, real estate agencies, telecomm companies, are there any industry standards in terms of when SINs are requested?

Increasingly in the US, individuals are asked for the SSN in the context of petty purchases, such as signing up for an account at a movie rental store. Technically, the movie rental store considers the lending of a title an extension of credit, thus justifying the collection of the SSN. However, these movies are worth a small amount of money, and in requiring the individual's SSN to rent them, the business passes on risk to the consumer in the form of security breaches and identity theft. There must some limit to the power of institutions to treat trivial provision of products or services as an extension of credit. For instance, individuals should be able to pay a security deposit to start utilities and other services without giving away their SSN.

9. What would be the costs associated with developing a unique identifier? How long would it take to implement this?

No comment.

10. Would truncating the SIN be a preferred solution? If so, how could that be implemented?

No. The underlying problem with the use of the SIN by consumer reporting agencies is not limited to the printing of the SIN on the credit report. The problem arises from the maintenance of a database of information linked to the individual's SIN.

In the US, it isn't clear whether there is a truncation standard. We have heard reports that some companies limit access to the first five numbers of the SSN, while in other cases, companies only obscure the last four digits.

Option IV – Allow consumers to place freezes on their credit reports

Upon a consumer's request, credit bureaus must place a freeze on the consumer's credit report free of charge. If a freeze is in place, the credit bureau would not be permitted to release the credit report to a third party without prior express authorization from the consumer. Authorization may be obtained by contacting the consumer at a predetermined telephone number or street address.

1. Do you think this option would better protect against identity theft. Why or why not?

Yes. This option would make it easier for consumers to prevent identity theft. We have attached a paper that discusses the merits of credit freeze in detail.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

Credit bureaus should bear the costs of verifying an individual's identity prior to the release of personal information.

3. Should there be exemptions? If yes, what type?

No. All individuals should have the ability to request that a freeze be placed on his or her credit report. In some states, only victims of identity theft can place a freeze.

4. Should there be a penalty associated with this provision?

Yes, there should be a penalty if a consumer reporting agency fails to implement a credit freeze immediately after a consumer's request.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

If a report is released in violation of the freeze, resulting in identity theft, the consumer reporting agency should be liable for losses.

6. Are there disadvantages for consumers or industry? Please describe.

Please see attached paper.

7. Should this be offered as a preventive and/or post theft instrument?

Preventive. An individual should not have to be a victim of identity theft to protect his or her information. Credit freeze is extremely useful as a prophylactic tool for individuals not likely to request credit, such as the elderly and children. Unfortunately, both populations—even toddlers—are victims of identity theft under the US system.

8. Are there implications for monitoring of credit worthiness and other marketing activities?

A credit freeze should indicate to consumer reporting agencies that the individual does not want to receive additional pre-screened marketing offers.

Additionally, we think credit monitoring should be free for interested consumers. Consumers have very little incentive to access their credit report unless they fear inaccuracy. But consumer reporting agencies have seized on individuals' fear to market their monitoring services and their services are benefited by these possible inaccuracies. The more inaccuracies or chance of inaccuracies a report, the more the credit service provider can persuade the consumer that the service is necessary because no one can prove or correct an inaccuracy without accessing a report.

Credit reporting agencies are required to pursue reasonable procedures to guarantee "maximum possible accuracy."[15] By continuing to market by exacerbating consumer fear and charging for a service to monitor their own mismanagement of credit data, credit reporting agencies are violating this "very high standard set by statute."[16] Far from charging consumers for the credit monitoring service, credit reporting agencies should be providing it for consumers without charge. In order to fulfill the statutory requirement of maximum possible accuracy, credit reporting agencies are duty-bound to provide consumers with a way to ensure the accuracy of their reports. By the mere existence of the credit monitoring services, it is shown that such services are technologically and economically feasible to convey to consumers the status of their credit on an on-going basis. Thus, the credit reporting agencies are aware that there are steps available to improve and assure the accuracy of the reports they maintain, and with this awareness comes the obligation to take such steps.[17] Consumers must have constant access to their reports if credit reporting agencies continue to share information and update credit files based on affiliate sharing or other information sources. Consumers should not be required to compensate credit reporting agencies for fulfilling their statutory duty, especially because the monitoring service infrastructure is already in place and functioning, operated by the credit reporting agencies themselves. Therefore, in order to assure accuracy-the maximum possible accuracy required by statute-credit reporting agencies should cease their statutory infringing practices and provide credit monitoring services to consumers without charge.

9. Should there be any exceptions to the freeze on credit reports?

Certain parties, such as companies that currently have an account with the consumer, should be able to access the report for account review purposes.

---

[15] 15 U.S.C. § 1681(e)(b) (2005).
[16] *Andrews v. TRW Inc*., 225 F.3d 1063 (9th Cir. 2000), *rev'd on other grounds*, 534 U.S. 19 (2001).
[17] FTC Official Staff Commentary § 607 item 3B (1995).

10. Should there be a reasonable cost-recovery fee chargeable for this service?

No.

Option V – Require organizations that store personal information to notify individuals and credit bureaus in cases of security breaches

When the security of personal information held by an organization is breached, the organization must contact the individuals whose personal information has been compromised as well as relevant credit bureaus as soon as reasonably possible

1. Do you think this option would better protect against identity theft. Why or why not?

Yes. Since the California legislation required that individuals be notified of security breaches, the extent of the problem of unauthorized access of personal information has been revealed.[18] Organizations many not have a sufficient incentive to disclose a security breach without the legislation. The cost of notifying consumers creates an incentive for organizations to improve their security. Moreover, the option empowers consumers with information about an organizations previous security breaches prior to disclosing his or her information to an organization. Because this option will create some risk for organizations failure to protect personal information, organizations may become less likely to retain personal information that they no longer need

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

Consumers could benefit from notification by taking preventative steps, such as credit freeze, to avoid identity theft.

3. Should there be exemptions? If yes, what type?

The California standard provides no exemption for giving security breach notices.

4. Should there be a penalty associated with this provision?

The penalty associated with failure to give notice of breach should be sufficient to prevent businesses from choosing a to risk receiving a fine over giving notices to consumers.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

Both the individuals' responsible for the data breach and the impostor who steals identities should be liable.

6. Are there disadvantages for consumers or industry? Please describe.

The Committee should be sceptical of claims that notices of security breaches create a disadvantage in that consumers will come to ignore the warnings. Some consumers are going to choose not to take action, or to simply throw away the notice. This should not result in other individuals being placed at heightened risk without notice of the problem.

7. Are there any market place incentives, i.e. contractual obligations that require organizations to disclose when they have had a breach of security? If so, what are they and do they pertain solely to breaches of specific information, i.e. financial breaches?

No comment.

---

[18] *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the Choicepoint Incident, available at http://www.privacyrights.org/ar/ChronDataBreaches.htm

8. As a consumer, would you be willing to give up some control over your personal information by allowing a company to put a fraud alert on your credit bureau file in a timely way to protect you from identity theft?

We do not see the placement of a fraud alert on a consumer's file as a loss of control over personal information. Under the US statutory scheme, a fraud alert places *more* control over personal information than the default standard.

9. What should be the threshold for notifying the consumer that personal information has been breached?

The California standard creates an obligation to give notice whenever unauthorized access to personal information has been detected.

10. Within what period of time, and by what means, should companies have to notify consumers?

Companies could give individuals a choice concerning the method of notice. In absence of the individual's direction, first class mail should be used. It is important that these mailpieces are designed to attract the individual's attention (In *AT&T v. Ting*, it was shown that AT&T actually performed market research to determine how to design a letter so that the company's customers would not read it[19]).

11. Should this proposal include a duty for the organization to notify PhoneBusters National Call Centre?

There should be notice to a government agency that can track security breaches statistically and release information to the public concerning the state of security. Prior to the California security disclosure law, consumers could only rely upon public relations statements concerning security of their personal information. Often, these representations were breathless and lacked in substantive information. For instance, Charles Morgan, the CEO of data broker Acxiom, testified to the Federal Trade Commission that the company's security was exceptional and multi-tiered. Within a year, two different individuals were able to crack the company's system, accessing 20 million records. The methods to break the system were simple, and demonstrated that the company's security was exceptionally bad.

Simply put, without this information, consumers will continue to have to rely upon unsubstantive and misleading statements of public relations departments rather than real data.

12. Is this a good approach to achieving a centralized reporting organization that can detect trends and compile more accurate statistics?

For the reasons stated above, we believe that central reporting will result in more accurate statistics that the current system.

[19] 182 F. Supp. 2d 902 (2002).

Option VI – Require credit bureaus to place fraud alerts on consumers' credit reports in cases of security breaches or upon the request of an identity theft victim

Upon receiving notice from an organization that the security of the victim's personal information has been breached, or upon request by an identity theft victim, a credit bureau must place a fraud alert on the consumer's credit report that his or her identity may have been used without consent to fraudulently obtain goods or services. A creditor that receives a credit report with such a notice must not give or extend credit in the person's name without first taking reasonable steps to verify the identity of the credit applicant.

1. **Do you think this option would better protect against identity theft. Why or why not?**

Yes, this option will help protect identity theft by streamlining the process that the consumer uses to place a fraud alert. However, the standard proposed once a fraud alert is issued—that the creditor that receives a report with a fraud alert must take "reasonable steps to verify the identity of the credit applicant," is too weak. It suggests that reasonable steps to verify the identity are not necessary absent indicators of fraud. A better approach would be to put the burden on creditors to always take reasonable steps (at least) to authenticate the customer. In situations where fraud is suspected, there should be a heightened duty of care in order to prevent identity theft.

We also comment that the length of a fraud alert should be extended. In the US, three different levels of fraud alerts are available—90 days, 2 years (for active duty military personnel only), and 7 years. The 90 day freeze is too short, as identity theft can happen months or years after data are stolen. The 7 year freeze is too difficult to consumers to exercise, as it requires that the consumer obtain a police report, which is difficult in some jurisdictions. Consumers should be able to obtain a fraud alert that is longer than 90 days without obtaining a police report.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

There should be no cost to place a fraud alert on a consumers file.

3. Should there be exemptions? If yes, what type?

No.

4. Should there be a penalty associated with this provision?

Yes, there should be a penalty for failing to place a fraud alert on a consumer's credit report after receiving a request from a consumer to do so.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

Individuals who lend credit to impostors should be liable for losses associated with identity theft where the creditor failed to exercise proper care in authenticating the customer.

6. Are there disadvantages for consumers or industry? Please describe.

We think that stronger fraud alerts will result in benefits to consumers.

Option VII – Require credit lenders to disclose details of fraudulent debts to victims

Upon request, credit lenders must provide identity theft victims with details regarding the fraudulent debt that was incurred in their name.

1. Do you think this option would better protect against identity theft. Why or why not?

Yes, this option will help consumers. However, it is important that businesses are educated about these requirements. In the United States, FACTA allows victims to go to a business that lent credit in their name, and obtain the business records associated with the transaction. Unfortunately, victims in the United States often have not been able to access their records because businesses are unfamiliar with the requirement. Many businesses will not hand over the records, despite the FACTA statute, without a subpoena.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

The business that enabled the identity theft should bear the cost of producing the records. These records are not likely to be voluminous (it usually consists of a credit application and copies of identification information), and therefore costs should not be extensive.

3. Should there be exemptions? If yes, what type?

No comment.

4. Should there be a penalty associated with this provision?

The US experience has been that many companies will not comply with the provision without a subpoena. There should be a penalty to simply ensure that businesses comply with the provision without inconveniencing the victim.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

Individuals who lend credit to impostors should be liable for losses associated with identity theft where the creditor failed to exercise proper care in authenticating the customer.

6. Are there disadvantages for consumers or industry? Please describe.

Because many police departments will not investigate identity theft crimes, there are many advantages to this requirement to consumers who hire a private investigator or investigate the crime on their own. The credit application can provide clues to the identity of the impostor. This provision will assist individuals in catching identity thieves.

Option VIII – Require credit bureaus to block information about fraudulent debts appearing on a consumer's credit report

Upon receipt of proof of identity theft, a credit bureau must block information about debts incurred in a consumer's name by an identity thief from being reported in the consumer's credit report. A credit bureau may deny or rescind a block in certain circumstances. If the block is denied or rescinded, the bureau must notify the consumer of their decision to do so and provide reasons for their decision.

1. Do you think this option would better protect against identity theft. Why or why not?

This option would better protect consumers who were the victims of identity theft by facilitating the restoration of their credit rating. A number of consumers in the United States report having difficulty removing fraudulent information from their credit reports.

As part of this option, credit bureaus should provide free credit monitoring to victims of identity theft.

Finally, to facilitate early detection of identity theft, a consumer should be notified of any change that is made to information held in her or her file by the credit bureau. In the US, there is a requirement that furnishers disclose to consumers that they can provide negative information to the consumer reporting agency. However, furnishers may do this at any time, and thus many comply with the requirement by putting a notice in a cardholder agreement. As a result, this requirement has given consumers little benefit in the US. It should be fixed by a requirement that the furnisher provide notice when it is submitting negative information to the consumer reporting agency.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

Consumers who are the victims of identity theft should not be penalized by having to pay to remove debts falsely created in their name. Consumer reporting agencies should bear the cost of blocking negative information.

3. Should there be exemptions? If yes, what type?

No.

4. Should there be a penalty associated with this provision?

Yes. An organization that fails to investigate and remove a bad debt after being notified by the consumer that the debt does not belong to him or her should be penalized.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

In cases where individuals lose the opportunity to gain a mortgage, for instance, because a consumer reporting agency failed to block false negative information, the consumer reporting agency should be liable for the loss.

6. Are there disadvantages for consumers or industry? Please describe.

No comment.

7. Should information be blocked based on the consumer submitting the identity theft statement? Alternatively, should there be time for the credit bureau to verify facts with the credit lender before blocking the information?

In some cases, individuals will falsely disclaim debt. There has to be a method for determining which cases are legitimate and which are false. If there are strong indications of fraud, a consumer reporting

agency can flag the debt as disputed. But where dispute appears legitimate, the information should be blocked.

8. Blocked information may need to be retained on file for investigation purposes. But, at what point should information that is blocked be completely removed from the file?

Blocked information should be removed as soon as the credit bureau has verified that the information is incorrect. Consumers should not face the risk that false information is inadvertently included in their file.

9. Should blocks be streamlined such that when information is blocked at one credit bureau, it is handled in the same way at other credit bureaus? Alternatively, should there be one central clearing agency for handling consumer requests to block information about debts incurred by identity thieves?

Consumers should not have to file separate applications identifying bad debts with each credit bureau.

Option IX - Make organizations liable for damages

Organizations would be liable for damages for failing to comply with the following proposals:

A. Creditors must:

(a) Contact consumers at a pre-designated telephone number before issuing credit, where there is a fraud alert on the credit file,

B. Credit bureaus must:

(a) Properly verify the identity of someone accessing a credit report, or
(b) Put a freeze on consumers' credit report in accordance with the provisions set out in Option 4,
(c) Put a fraud alert on the file where requested to do so in accordance with the provisions set out in Option 6,
(d) Block information in accordance with the provisions set out in Option 8.

C. All Organizations must:

(a) Truncate payment card numbers in accordance with the provisions set out in Option 1,
(b) Notify people affected by a security breach in accordance with the provisions set out in Option 5.

All these organizations would be legally responsible for damages suffered by identity theft victims if they fail to comply with these measures.

1. Do you think this option would better protect against identity theft. Why or why not?

Yes, financial penalties are necessary to ensure proper handling of individual's personal information. A statutory penalty is likely necessary because courts in the United States have been reluctant to assign liability to credit granting companies for failing to protect an individual's personal information.

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

No comment.

3. Should there be exemptions? If yes, what kind?

Exemptions should be time-limited, to ensure full compliance with the requirements of the law.

4. For this option, who should ultimately be responsible for losses incurred from identity theft?

Consumer reporting agencies should be liable for failing to observe specified duties. Individuals who lend credit to impostors should be liable for losses associated with identity theft where the creditor failed to exercise proper care in authenticating the customer.

5. Are there disadvantages for consumers or industry? Please describe.

No comment.

Option X – Inform victims of their rights

Organizations must make information about victim's rights readily available. Repairing the effects of identity theft is a costly and time-consuming process. Victims need information in plain language that tells them how to settle fraudulent debts and correct their financial and credit records.

1. Do you think this option would better protect against identity theft. Why or why not?

Yes, it is important to inform victims quickly of the process to settle fraudulent debts. It is important to closely oversee the language employed by businesses to describe individuals' rights.[20]

2. What would be the costs / savings of such an initiative? Who should pay for the costs, if any?

No comment.

3. Should there be exemptions? If yes, what kind?

No comment.

4. Should there be a penalty associated with this provision?

Penalties should be in place to ensure compliance.

5. For this option, who should ultimately be responsible for losses incurred from identity theft?

No comment.

6. Are there disadvantages for consumers or industry? Please describe.

No comment.

7. Should organizations be required to have a toll-free number for this purpose?

Yes.

8. What type of information would be required to provide, e.g. dispute resolution process, how to prevent further ID theft (alerts, freezes, blocking of information), identity theft statement, contact names and numbers, etc?

All the categories of information listed would assist individuals in addressing identity theft.

---

[20] *See Ting v. AT&T* , 182 F. Supp. 2d 902 (2002)(defendant phone company designed notices so that consumers would not read them).

9. Should a separate centralized agency be set up for this purpose? Should such an agency also help facilitate requests for fraud alerts following security breaches, freezes on credit reports and the blocking of negative information in a streamlined manner?

An office of identity theft prevention and resolution would assist individuals in addressing the crime. Such an entity could collect individuals' complaints, generate statistical data, and make recommendations for additional reforms.

Please attach any additional comments you may wish to convey.

Thank you for your participation in this consultation.