Vermont Department of Banking, Insurance, Securities and Health Care Administration

BISHCA BULLETIN 1
December 21, 2007

Security Breach Notification Guidance

This Guidance describes the steps that a person or entity licensed or registered with the Vermont Department of Banking, Insurance, Securities and Health Care Administration (the "Department") should take in the event that its computerized data or systems containing "personal information", as set forth in the Vermont Security Breach Notification Statute, have been subject to a security breach[1]. The Department encourages businesses to develop a security breach policy and to communicate the policy to its employees.

The recommendations offered in this guidance are neither regulations, nor mandates, nor legal opinions. Rather, the recommendations are a contribution to the development of "best practices" for those licensed or registered with the Department to follow in the event of a security breach.

The Vermont Security Breach Notification Act, codified at 9 V.S.A. Sections 2430 and 2435, became effective on January 1, 2007. This law requires businesses to notify consumers in the event that the business suffers a "security breach". A security breach is defined as the unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the business, however, it does not include the good faith but unauthorized acquisition or access of personal information by an employee or agent for a legitimate purpose of the data collector, provided the personal information is not used for purposes unrelated to the data collector's business or subject to further unauthorized disclosure. 9 V.S.A. Section 2430(8).

"Personal information" that is subject to the law is defined as:

> an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data

[1] The Guidance does not apply to a financial institution, bank, or credit union that is subject to either (A) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision or (B) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration, as such federal guidance may be revised or amended from time to time.

elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) Social Security number;
(ii) Motor vehicle operator's license number or nondriver identification card number;
(iii) Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
(iv) Account passwords or personal identification numbers or other access codes for a financial account.

9 V.S.A. Section 2430(5).

A business should begin taking action as soon as it suspects that a security breach has occurred. Obviously, if the business discovers there has been no security breach, then neither the statue nor this guidance apply. If it appears that a security breach has occurred, however, the business should immediately begin taking appropriate action to contain the breach and to promote and protect individual privacy interests.

The statute requires that notice be sent to affected consumers following discovery of or notification about the breach "in the most expedient time possible and without unreasonable delay", consistent with the needs of law enforcement. 9 V.S.A. Section 2435(b).

Generally, early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information and protect themselves against identity theft. While the Vermont law on notice of security breaches only applies to unencrypted computerized data, the Department recommends that businesses also consider applying these guidelines to records maintained in any media, including paper records.

A business should take the following steps if it suffers a security breach. The business should review all steps immediately, and take as many of the detailed steps as possible, as quickly as possible. Unlike many "best practices", however, the following steps do not contain all of the practices that should be observed and, based upon the specific circumstances, the business may need to take additional or alternative action to protect the consumer's personal information.

1. Secure the data immediately.

a. Call your head of computer operations or information technology, or other appropriate information technology personnel, to find out what steps must be taken to secure the data. Take all appropriate measures to secure the data, including possibly taking the computer server off line or isolating the data.

b. Exercise extreme caution in any attempt to determine whether the data has been compromised until law enforcement has approved the steps you plan to take. Failure to exercise such caution could result in the loss or contamination of evidence.

c. Appendix 1 contains a description from law enforcement of some of the steps a business should take to secure the data in the event of a security breach.

2. Involve Law Enforcement immediately.

a. A business that has suffered a security breach should involve law enforcement immediately. As noted above, failure to do so could result in the loss or contamination of evidence. Call the state police, FBI, and/or other applicable law enforcement to report the incident and determine next steps. If you are a Vermont-based business, or the data at issue is housed in Vermont, call:

State Police: Bureau of Criminal Investigations
802-241-5350

FBI: During normal business hours, call the Burlington FBI office at 802-863-6316

After business hours, call the Albany FBI office at 518-465-7551

If your business is located out of state and the data at issue is housed out of state, call the FBI, state police, or other appropriate law enforcement agency in your area.

b. Inform law enforcement of your desire to notify consumers of the breach within ten business days. If law enforcement requests a delay in notification for purposes of a law enforcement investigation, the request must be made in writing or you must document the request contemporaneously, noting the name of the law enforcement officer making the request and the name of the officer's agency.

c. If law enforcement requests a delay in notification for purposes of a law enforcement investigation, prepare a rough draft of your notification to consumers so that you can complete preparation of the notices and send them immediately upon hearing that the delay is no longer needed.

d. The law enforcement agency making a request for delay is responsible for promptly notifying you when the law enforcement agency believes that

delay will no longer impede the law enforcement investigation. Until you are notified that the delay is no longer needed, maintain contact with the responsible law enforcement officer at reasonable intervals (for example, approximately every two to three weeks) to determine that the delay is still required. It should not be necessary for law enforcement to complete its investigation before notice can be sent to affected consumers.

e. After the law enforcement agency notifies you that the delay is no longer needed, send your notice to consumers as soon as possible.

3. Contact any entities from which you may have obtained the data immediately.

a. If you received the data from other entities, such as banks or other businesses, contact these entities as they may have their own obligations to notify consumers about the security breach.

4. Notify the Vermont Department of Banking, Insurance, Securities and Health Care Administration about the breach.

a. Call and inform the Department about the breach by contacting:

BISHCA General Counsel at 802-828-3301

5. Notify consumers about the breach in the most expedient time possible and without unreasonable delay, typically within 10 business days of discovery.

a. If law enforcement does not request a delay in notification to consumers, you must notify consumers about the breach in the most expedient time possible and without unreasonable delay. Typically, the Department would expect the business to notify consumers within 10 business days following discovery of the breach.

b. The notice should contain the following information:

- A general description of the unauthorized access or acquisition.
- The type of personal information affected.
- A general description of the steps you will take to protect the information from further unauthorized access or acquisition.
- A toll-free telephone number that consumers may call for further information and assistance.
- Advice that directs the consumer to remain vigilant by reviewing account statements and obtaining and monitoring free credit reports from each credit reporting agency to determine if there is suspicious activity, such as new accounts being opened in the

consumer's name. [For example, consumers in Vermont are entitled to two free credit reports each year from each credit reporting agency. The Attorney General's website has information about free credit reports available to Vermonters: http://www.atg.state.vt.us/upload/1120132977_How_to_Get_Free_Credit_Reports.pdf]

c. A sample letter is provided in Appendix 2. The sample letter is a guide designed for use when you do not know whether the consumer's information has been misused and may be modified to fit your particular circumstances. If you are aware that the consumer's information has been misused, you should send a more specific letter outlining how the information has been misused and recommending that the consumer take immediate action to guard against identity theft.

d. Consider whether you will offer credit monitoring services to the consumers. These are services offered by credit reporting agencies to determine if there is suspicious activity such as new accounts being opened in the consumer's name. While not required by law, many companies that experience breaches provide credit monitoring services to consumers.

e. Send the notice in one of the following ways.

1. Direct notice to consumers through:

i. A mailing to the consumer's residence; or

ii. The telephone, provided the telephone contact is directly made with each consumer, and not through a pre-recorded message; or

iii. Electronic notice via email (Note: it is difficult to qualify to use electronic notice. See 9 V.S.A. Section 2435(b)(5)(A)(ii).);

2. Substitute notice is allowed if you can demonstrate one of the following:

(1) providing direct notice through the mail or telephone would cost more than $5,000;

(2) the group of consumers affected by the security breach exceeds 5,000; or

(3) the data collector does not have sufficient contact information to provide notice via the mail or telephone.

If you satisfy one of the three criteria for substitute notice, then you may provide notice to affected consumers by doing **both** of the following:

i. prominently placing the notice on your website if you have one; **and**
ii. sending a press release with all the information to be contained in the notice to major statewide and regional media.

f. Whichever mechanism of distribution you use, the notice must contain all the elements outlined in 4.b above.

6. **Notification of the three major credit reporting agencies.**

A breach involving a large number of individuals can have a significant impact on consumer reporting agencies and their ability to respond efficiently. Therefore, except as set forth below, you should notify the consumer reporting agencies when you send out notices to more than 1,000 consumers.

The section of the Vermont Security Breach Notification Act that requires notification to major credit reporting agencies, 8 V.S.A. §2435(c), does not apply to a person or entity licensed by or registered with the Department under Title 8 V.S.A. The Department, however, strongly encourages the business to notify the consumer reporting agencies in the event notices are sent to more than 1,000 consumers. (The Department is aware that many of the businesses licensed or registered under Title 8 are significant users of credit reporting agency services and may have established other procedures and other specific contacts with the agencies to notify them in the event of a security breach.)

The general contact information for the three major credit reporting agencies is:

- **Equifax**

U.S. Consumer Services
Equifax Information Services, LLC
Phone: 678-795-7971
Email: businessrecordsecurity@equifax.com

- **Experian**

Experian Security Assistance
P.O. Box 72
Allen, TX 75013
Email: BusinessRecordsVictimAssistance@experian.com

- **TransUnion**

Phone: 1-800-372-8391

Email: fvad@transunion.com

7. Notice of a security breach is not required if you determine that misuse of personal information is not reasonably possible, and you so inform the Department.

a. If you establish that misuse of the data is not reasonably possible, then you may forgo notifying affected consumers about the breach *as long as* you provide a detailed explanation of your determination to the Department. The Department expects that, in most instances, the detailed explanation will be provided within 10 business days following the discovery of the breach. The explanation should be sent to the following: Vermont Department of Banking, Insurance, Securities and Health Care Administration, Attn: General Counsel, 89 Main Street, Montpelier, Vermont 05620-3101.

b. You may designate your explanation as "trade secret" if it meets the definition of trade secret under 1 V.S.A. Section 317(c)(9).

c. If you learn, after notifying the Department, that misuse of the personal information has occurred or is occurring, then you must provide, pursuant to 9 V.S.A. §2435(d)(2), notice of the security breach to affected consumers in the most expedient time possible and without unreasonable delay, typically within 10 business days of receiving such information.

Dec. 21, 2007
Date

s/PJT
Paulette J. Thabault, Commissioner

Appendix 1

Procedures the Computer User Should Institute Both Prior to Becoming a Computer Crime Victim and After a Violation Has Occurred

Guidance from the FBI National Computer Crime Squad
www.emergency.com/fbi-nccs.htm

· Place a login banner to ensure that unauthorized users are warned that they may be subject to monitoring.

· Turn audit trails on.

· Consider keystroke level monitoring if adequate banner is displayed.

· Request trap and tracing from your local telephone company.

· Consider installing caller identification.

· Make backups of damaged or altered files.

· Maintain old backups to show the status of the original.

· Designate one person to secure potential evidence

· Evidence can consist of tape backups and printouts. These should be initialed by the person obtaining the evidence. Evidence should be retained in a locked cabinet with access limited to one person.

· Keep a record of resources used to reestablish the system and locate the perpetrator.

Reporting a Computer Crime to Law Enforcement

Guidance from the California Highway Patrol Computer Crimes Investigation Unit
www.chp.ca.gov/html/computercrime.html

When reporting a computer crime be prepared to provide the following information:

· Name and address of the reporting business.

· Name, address, e-mail address, and phone number(s) of the reporting person.

· Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).

· Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.).

· Description of the incident.

· Date and time the incident occurred.

· Date and time the incident was discovered.

· Make/model of the affected computer(s).

· IP address of the affected computer(s).

· Assigned name of the affected computer(s).

· Operating System of the affected computer(s).

· Location of the affected computer(s).

Incident Response DOs and DO NOTs

DOs

1. Immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.

2. Use the telephone to communicate. Attackers may be capable of monitoring E-mail traffic.

3. Immediately notify an appropriate law enforcement agency.

4. Activate all auditing software, if not already activated.

5. Preserve all pertinent system logs, e.g., firewall, router, and intrusion detection system.

6. Make backup copies of damaged or altered files, and keep these backups in a secure location.

7. Identify where the affected system resides within the network topology.

8. Identify all systems and agencies that connect to the affected system.

9. Identify the programs and processes that operate on the affected system(s), the impact of the disruption, and the maximum allowable outage time.

10. In the event the affected system is collected as evidence, make arrangements to provide for the continuity of services, i.e., prepare redundant system and obtain data back-ups. To assist with your operational recovery of the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

DO NOT

1. Delete, move, or alter files on the affected systems.

2. Contact the suspected perpetrator.

3. Conduct a forensic analysis.

Appendix 2

Sample Notification Letter

SAMPLE LETTER
For Use When The Breached Entity Does Not Know Whether the Consumer's Information Has Been Misused

Dear :

We are writing to you because of a recent security incident at *[name of organization]. [Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]*

Below is a checklist of suggestions of how you can best protect yourself in this situation.

1. **Review your bank, credit card and debit card account statements** over the next twelve to twenty-four months and immediately report any suspicious activity to your bank or credit union.

2. **Monitor your credit reports** with the major credit reporting agencies.

Equifax	Experian	TransUnion
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740241	P.O. Box 2104	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Under Vermont law, you are entitled to a free copy of your credit report from those agencies every twelve months. *[If you are offering consumers credit monitoring services, insert description of the services and instructions on how to access them.]*

Call the credit reporting agency at the telephone number on the report if you find:

- Accounts you did not open.
- Inquiries from creditors that you did not initiate.
- Inaccurate personal information, such as home address and Social Security number.

3. If you do find suspicious activity on your credit reports or other account statements, call your local police or sheriff's office and **file a report of identity theft**. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.

4. If you find suspicious activity on your credit reports or on your other account statements, consider placing a **fraud alert** on your credit files so creditors will contact you before opening new accounts. Call any one of the three credit reporting agencies at the number below to place fraud alerts with all of the agencies.

Equifax	Experian	TransUnion
800-525-6285	888-397-3742	800-680-7289

5. If you find suspicious activity on your credit reports or on your other account statements, consider placing a **security freeze** on your credit report so that the credit reporting agencies will not release information about your credit without your express authorization. A security freeze may cause delay should you wish to obtain credit and may cost some money to get or remove, but it does provide extra protection against an identity thief obtaining credit in your name without your knowledge. If you have Internet access and would like to learn more about how to place a security freeze on your credit report, please contact the Vermont Attorney General's website at:
http://www.atg.state.vt.us/display.php?smod=198

You may also get information about security freezes by contact the credit bureaus at the following addresses:

Equifax:

https://www.econsumer.equifax.com/consumer/sitepage.ehtml?forward=elearning_credit15

Experian:

http://www.experian.com/consumer/security_freeze.html

TransUnion:

http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page

If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

6. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you **check your credit report** for the next two years. Just call one of the numbers in paragraph 2 above to order your reports or to keep a fraud alert in place.

Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at http://www.atg.state.vt.us. Another helpful source is the Federal Trade Commission website, which you may find at http://www.ftc.gov/bcp/edu/microsites/idtheft/.

If there is anything *[name of your organization]* can do to assist you, please call *[toll-free phone number]*.

[Closing]