A CU*ANSWERS WHITEPAPER

MARCH 2013

CREDIT UNION LIABILITY FOR CONSUMER NOTIFICATION

March 12, 2013

There are many factors for deciding whether to notify consumers and under what circumstances. Credit Unions need to look at the consumer notification laws in the states where members reside and determine on a case-by-case basis whether consumers require notification.

CU*ANSWERS
A Credit Union Service Organization

AuditLink
CU*ANSWERS Management Services

GAME OVER

(FOR THE CONSUMER)

On April 19, 2011, Sony's PlayStation Network was shut down without warning. On April 20, Sony acknowledged that parts of the Network were down and that enhancements were needed to get the network up in a couple of days. Sony then spent a week brushing aside the increasingly furious complaints from their subscribers. On April 25, Sony informed consumers that "enhancements" were needed with no estimated time of completion. Finally on April 26, Sony came clean and admitted that their Network had been hacked. As many as 77 million subscribers were potential victims of the security breach. The Sony breach is thought to be largest such breach in history. Sony offered insurance and free games as a result of the outage. Unsatisfied with the Sony response, especially with respect to the delay in notifying consumers of the breach, hundreds of consumers filed a class action. Sony filed a motion to dismiss the case.

In 2012, the judge agreed with Sony and dismissed most of the allegations. The judge found that "increased risk" of identity theft was not enough; that the plaintiffs needed to show that they were *actually harmed* as a result of the Network hack. Economic damages suffered by subscribers, such as credit monitoring, loss of use of the Network services, and diminution of their gaming consoles was not enough to sustain a negligence claim. (The judge did grant the plaintiffs the right to amend the complaint in light of the ruling).

The court also dismissed arguments that Sony violated actionable consumer protection laws, was in breach of contract, or misrepresented the quality of its network security. Before registering for the Network all Plaintiffs had to agree to Sony's Privacy Policy, which states that

"there is no such thing as perfect security . . . we cannot ensure or warrant the security of any information transmitted to us . . ."

The judge stated that the presence of clear admonitory language that Sony's security was not "perfect," meant no reasonable consumer could have been deceived about the quality of Sony's network security.

As to the claim that Sony violated California's Breach Act, the court noted it was a complete defense for a company to send amended notifications out after the original notification was sent, as long as the amended notifications were sent out within 90 days and that the company's failure to send out correct information the first time was due to intention or reckless behavior. Without this showing, the plaintiff's claims were dismissed. ◆

NOTIFICATION LAW OVERVIEW

The Sony case illustrates a good general rule, in that the absence of *actual harm* suffered by the consumer as a result of security breach means the mere failure to notify alone is usually not enough to sustain a lawsuit. Indeed, most states do not allow consumers a private right of action for failure to notify, but rather reserve the right of the state to levy fines for failure to comply with notification laws. So while consumers may sue a financial institution for actual consequences of the breach, the failure to notify itself is normally not actionable. To be compliant, most financial institutions need to determine the likelihood of actual harm to a consumer in the event of a breach, and failure to assess may violate statutory requirements. False statements about security may be actionable, and credit unions may be in serious trouble with the FTC for COPPA violations.

Of course, failure to have consumer notification procedures in event of a breach, or failure to follow these procedures may cause a credit union to be out of compliance and at risk for adverse action by a regulatory authority. ◆

GRAMM-LEACH-BLILEY ACT

The Gramm-Leach-Bliley Act has as part of Section 501 a requirement that financial institutions have a consumer notification response as part of their information security program. The Act does not, however, specify when and under what circumstances members must be notified. It is likely, however, that the same negligence standard of ordinary care applies to financial institutions who fail to notify consumers in a timely manner. Failure to comply with Section 501 is unlikely to be dispositive in any case, but will be damaging to the financial institutions defense. In support of the FFIEC's guidance, the NCUA issued a letter in 2006 stating "policies and procedures should be in place to report unauthorized access to local law enforcement, your NCUA Regional Director, and members, if the analysis of the breach warrants member notification."

The Gramm-Leach Bliley Act implies and most state notification laws are specific that a business or individual may analyze the risk, and if the threat is minimal that the data will be used to harm the consumer, notice is *not required.* The standard will likely be ordinary care. ◆

STATE NOTIFICATION LAWS

There is no such thing as a federally mandated security breach notification law. There was an attempt to create one by Congress called the Safe Data Act, but it died in committee in 2011. As a result, all consumer notification laws are state-based and will vary. Four states have no consumer notification laws in the event of a security breach: Alabama, Kentucky, New Mexico, and South Dakota. Each credit union will need to look to their own law to determine notification requirements.

In Michigan, the notification requirements are set forth in the **Identity Theft Protection Act MCL 445.72**. To comply with the law, a Michigan credit union must determine, in good faith, whether or not the breach is likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of Michigan.

Note: A credit union that has members in more than one state would need to look at each state's notification laws to determine whether these members must be notified in event of a breach.

The language of the statute grants businesses in Michigan the opportunity to assess whether consumers will likely have substantial loss or identity theft prior to sending out a notification. The word "likely" is important to a Michigan business. A showing that a credit union conducted a full, fair, and independent investigation of the incident and honesty believed there was no threat to members will have a much better chance of defeating a negligence lawsuit. The duty imposed on a Michigan business is that of ordinary care.

Wisconsin law follows very similar logic. Notice in Wisconsin is not required when the acquisition of member information does not create a *material risk* of identity theft or fraud. Wisconsin businesses must make "reasonable efforts" to notify consumers. (**Wisconsin law 134.98 Notice of unauthorized acquisition of personal information**).

Michigan law requires notification to go out without "unreasonable delay." Michigan businesses can delay notification if additional time is required to assess the scope of the breach, or if law enforcement states that the notification will endanger national security.

Michigan prefers that the notice will go out in the mail, but allows for electronic, phone, and substitute notice to go out under certain circumstances. Substitute notice is allowed if notice must go to more than 500,000 residents or will cost $250,000 or more. Michigan businesses are also required to notify applicable consumer reporting agencies. Michigan credit unions are allowed to provide notice in accordance with regulatory requirements posted by the Federal Reserve or the NCUA.

Michigan has civil penalties if a credit union is shown to have violated MCL 445.72. However, Michigan law specifically prevents consumers from having a private right of action against a credit union for violations of this statute. So while financial institutions can be fined by the state, its consumers are barred from filing their own lawsuits against the credit union. Although consumers do not have the ability to file an independent claim for failure to notify, consumers may be able to use violations of MCL 445.72 against a credit union for failing in their duty to protect data. In theory, evidence of MCL 445.72 could be introduced if the failure to notify caused damage to the consumer. ◆

FALSE AND DECEPTIVE PRACTICES

Credit unions and other business can potentially be sued under consumer protection and other fraud laws if the institution makes a "false statement" or "deceptive practice." For example, Ziff-Davis Media was sued by several states when it declared that it had implemented better security after a breach, when it had done nothing of the sort. Ziff-David eventually settled with the states for $100,000 and paid each consumer $500 in restitution.

It could be considered a deceptive practice for a financial institution to claim it has or offers security practices that it does not and there is a breach. Such claims could come under the review of the Consumer Finance Protection Bureau and result in significant fines. ◆

COPPA

The Children's Online Privacy Protection Act prohibits the unauthorized collection of children's personal information online. Among the many requirements if children's data is to be collected online is obtaining verifiable parental consent prior to collecting, using, or disclosing children's personal information. Sony BMG ran afoul of COPPA in the use of their online music sharing service. The FTC claimed that on 196 of its Web sites, Sony BMG collected personal information from at least 30,000 underage children without first obtaining parental consent. Sony BMG also allowed children to interact with other Sony BMG fans, including adults, without their parents' knowledge, the FTC said. In the end, Sony BMG was required to pay $1,000,000 in fines. A credit union that suffers a breach of data that disclosed unauthorized information about children would be in serious trouble under COPPA. ◆

PROTECTED DATA

Definitions of what constitutes "protected data" may vary, but generally requires the individual's last name and first name/initial, *and* additional information account, social security, drivers license, credit card numbers, security codes, or biometric information. ◆

WHAT A BREACH NOTICE MUST CONTAIN UNDER MICHIGAN LAW

Michigan notices require the information to be written or communicated by phone in a clear and conspicuous manner. The notice must have the following information:

Describe the security breach in general terms.

Describe the type of personal information that is the subject of the unauthorized access or use.

If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches.

Include a telephone number where a notice recipient may obtain assistance or additional information.

Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft. ◆

MICHIGAN IDENTITY THEFT PROTECTION ACT (EXCERPT)

Act 452 of 2004

445.72 Notice of security breach; requirements.

(1) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state who meets 1 or more of the following:

(a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.

(b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

(2) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach.

(3) In determining whether a security breach is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state under subsection (1) or (2), a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.

(4) A person or agency shall provide any notice required under this section without unreasonable delay. A person or agency may delay providing notice without violating this subsection if either of the following is met:

(a) A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the agency or person shall provide the notice required under this subsection without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.

(b) A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the agency or person shall provide the notice required under this section without unreasonable delay after

the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.

(5) Except as provided in subsection (11), an agency or person shall provide any notice required under this section by providing 1 or more of the following to the recipient:

(a) Written notice sent to the recipient at the recipient's postal address in the records of the agency or person.

(b) Written notice sent electronically to the recipient if any of the following are met:

(i) The recipient has expressly consented to receive electronic notice.

(ii) The person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person or agency reasonably believes that it has the recipient's current electronic mail address.

(iii) The person or agency conducts its business primarily through internet account transactions or on the internet.

(c) If not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the person or agency if all of the following are met:

(i) The notice is not given in whole or in part by use of a recorded message.

(ii) The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person or agency also provides notice under subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within 3 business days after the initial attempt to provide telephonic notice.

(d) Substitute notice, if the person or agency demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed $250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state. A person or agency provides substitute notice under this subdivision by doing all of the following:

(i) If the person or agency has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents.

(ii) If the person or agency maintains a website, conspicuously posting the notice on that website.

(iii) Notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain additional assistance and information.

(6) A notice under this section shall do all of the following:

(a) For a notice provided under subsection (5)(a) or (b), be written in a clear and conspicuous manner and contain the content required under subdivisions (c) to (g).

(b) For a notice provided under subsection (5)(c), clearly communicate the content required under subdivisions (c) to (g) to the recipient of the telephone call.

(c) Describe the security breach in general terms.

(d) Describe the type of personal information that is the subject of the unauthorized access or use.

(e) If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches.

(f) Include a telephone number where a notice recipient may obtain assistance or additional information.

(g) Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

(7) A person or agency may provide any notice required under this section pursuant to an agreement between that person or agency and another person or agency, if the notice provided pursuant to the agreement does not conflict with any provision of this section.

(8) Except as provided in this subsection, after a person or agency provides a notice under this section, the person or agency shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the security breach without unreasonable delay. A notification under this subsection shall include the number of notices that the person or agency provided to residents of this state and the timing of those notices. This subsection does not apply if either of the following is met:

(a) The person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state.

(b) The person or agency is subject to 15 USC 6801 to 6809.

(9) A financial institution that is subject to, and has notification procedures in place that are subject to examination by the financial institution's appropriate regulator for compliance with, the interagency guidance on response programs for unauthorized access to customer information and customer notice prescribed by the board of governors of the federal reserve system and the other federal bank

and thrift regulatory agencies, or similar guidance prescribed and adopted by the national credit union administration, and its affiliates, is considered to be in compliance with this section.

…

(12) A person that provides notice of a security breach in the manner described in this section when a security breach has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable as follows:

(a) Except as otherwise provided under subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $250.00 for each violation, or both.

(b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $500.00 for each violation, or both.

(c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $750.00 for each violation, or both.

(13) Subject to subsection (14), a person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section.

(14) The aggregate liability of a person for civil fines under subsection (13) for multiple violations of subsection (13) that arise from the same security breach shall not exceed $750,000.00.

(15) Subsections (12) and (13) do not affect the availability of any civil remedy for a violation of state or federal law.

(16) This section applies to the discovery or notification of a breach of the security of a database that occurs on or after July 2, 2006.

(17) This section does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public.

(18) This section deals with subject matter that is of statewide concern, and any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of this state to regulate, directly or indirectly, any matter expressly set forth in this section is preempted.

CONSUMER SECURITY NOTIFICATION LAWS BY STATE

Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 et seq.
California	Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. 36a-701b
Delaware	Del. Code tit. 6, § 12B-101 et seq.
Florida	Fla. Stat. § 817.5681
Georgia	Ga. Code §§ 10-1-910, -911
Hawaii	Haw. Rev. Stat. § 487N-2
Idaho	Idaho Stat. §§ 28-51-104 to 28-51-107
Illinois	815 ILCS 530/1 et seq.
Indiana	Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.
Iowa	Iowa Code § 715C.1
Kansas	Kan. Stat. 50-7a01, 50-7a02
Louisiana	La. Rev. Stat. § 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10 §§ 1347 et seq.
Maryland	Md. Code, Com. Law § 14-3501 et seq.
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.
Michigan	Mich. Comp. Laws § 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	2010 H.B. 583 (effective July 1, 2011)
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 30-14-1704, 2-6-504
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq., 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21
New Jersey	N.J. Stat. 56:8-163

New York	N.Y. Gen. Bus. Law § 899-aa
North Carolina	N.C. Gen. Stat § 75-65
North Dakota	N.D. Cent. Code § 51-30-01 et seq.
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. § 74-3113.1 and § 24-161 to -166
Oregon	Oregon Rev. Stat. § 646A.600 et seq.
Pennsylvania	73 Pa. Stat. § 2303
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.
South Carolina	S.C. Code § 39-1-90
Tennessee	Tenn. Code § 47-18-2107, 2010 S.B. 2793
Texas	Tex. Bus. & Com. Code § 521.03, Tex. Ed. Code 37.007(b)(5) (2011 H.B. 1224)
Utah	Utah Code §§ 13-44-101, et seq.
Vermont	Vt. Stat. tit. 9 § 2430 et seq.
Virginia	Va. Code § 18.2-186.6, § 32.1-127.1:05
Washington	Wash. Rev. Code § 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98 et seq.
Wyoming	Wyo. Stat. § 40-12-501 to -502
District of Columbia	D.C. Code § 28- 3851 et seq.
Guam	9 GCA § 48-10 et seq.
Puerto Rico	10 Laws of Puerto Rico § 4051 et. seq.
Virgin Islands	V.I. Code § 2208

States with no security breach law: Alabama, Kentucky, New Mexico, and South Dakota.