

Shado

*Managing
an Effective
Identity Theft
Prevention
Program*

Past Experiences

Program Administration

Exam Preparation

Enter

BY JOHN P. BONORA, CRCM

wars

You have to admit that the commercials are fairly catchy.

High-powered marketing brain trusts have generated everything from singing pirates in restaurants to voiced-over elderly women sharing stolen credit card stories. In recent years, corporate America has added a level of humor to identity theft. But make no mistake: being an identity theft victim isn't funny. Most victims cringe at the sound of clever credit bureau jingles and cannot help but feel helpless when recalling their ordeals. This shadow war between the innocent consumer and the crafty fraudster has been waged for decades. Only in the mid-1990s did the Federal Trade Commission and Congress begin arming consumers with the information and tools they need to combat identity crimes. Tools such as information pamphlets, truncated transaction receipt requirements, credit profile fraud alerts, and a victim assistance Web site have all aided in the prevention of the crime.

In the past, many financial entities played a passive role in fighting identity theft. On November 1, 2008, the Fair Credit Reporting Act (FCRA) drastically changed that role as creditors and financial institutions alike were made responsible for executing formal identity theft prevention programs. Despite the recent turmoil within the finance industry, banks were required to remain focused on implementing functional programs by the required compliance date. With a little under a calendar year to prepare, organizations were thrust into the complex and rapidly evolving world of identity theft prevention. Although the requirements afforded institutions the opportunity to leverage existing resources, the development of a comprehensive program nonetheless proved challenging for professionals in the compliance arena. Compliance and risk officers across the country face the task of balancing effective controls to drive a successful program while not overwhelming business lines with duplicative procedures, timely documentary exercises, and costly IT systems. Program administrators also face unique obstacles surrounding oversight of service providers and the pioneering examination approach that certain regulators will utilize when assessing an institution's level of compliance.

Moving forward, every financial institution will be a critical player in this shadow war against identity theft. Understanding how to overcome these obstacles will be the key to managing an effective yet sustainable program for your institution.

Vendor Oversight

One of the most-debated red-flag topics among bankers and regulators is the requirement that resides in the “Administration of the Program”¹ section. Specifically, the requirement states that “Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must ... (4) exercise appropriate and effective oversight of service provider arrangements.”

It is unlikely that bankers gave this section much scrutiny when the proposed rule was first introduced during 2006. In fact, when the final rule was released, many financial institutions probably viewed this requirement as one area where a great amount of leveraging could occur. After all, vendor oversight is nothing new to the banking industry, and most banks have existing vendor management programs that have been structured in concert with Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and Office of the Comptroller of the Currency (OCC) guidance. However, when this requirement is coupled with the corresponding section in Appendix J to Part 334, the waters become a bit muddied. Every financial institution required

to implement a program must consider the guidelines established in Appendix J. Regarding vendor oversight, Appendix J provides an example of acceptable compliance. The example set forth in the “Oversight of Service Providers”² section essentially refers to a red-flag contract clause. While a red-flag contract clause is not required by the regulation, the guidelines have in essence created an expectation for federal examiners: that financial institutions will obtain the clause or addenda from applicable service providers.

In theory, this appeared to be reasonable. Authors of the regulation forecast an industry response similar

to that which occurred with the passage of the Gramm-Leach-Bliley Act (GLBA) and the subsequent release of the FFIEC’s *Interagency Guidelines Establishing Information Security Standards*. Within those guidelines, a financial institution must “enforce a contract with the company that requires it to implement appropriate measures designed to implement the *objectives* of the Security Guidelines.”³ In today’s environment, GLBA clauses in service provider contracts are virtually industry standard.

Unfortunately, some vendors do not appear to be as accommodating for the red-flag contract clause. There appear to be two reasons for this. First, it is not uncommon when a financial organization broaches this subject with a vendor that the vendor simply claims the regulation does not apply to their company. Remember, the red-flag regulation applies only to entities that offer or maintain covered accounts. Second, adding a red-flag contract clause requires

the service provider to assume an extensive amount of risk. Because the vendor is not legally required to offer the contract clause, there is no benefit to the vendor adding this clause during a contract cycle. Guaranteeing the prevention of identity theft or a data breach is virtually impossible, and as a result vendors will do anything to avoid adopting any portion of liability.

As contract cycles expire, vendors will be forced to adopt some type of red-flag clause to remain competitive in the marketplace. However, the clause will not be industry standard for several years, creating a short-term dilemma for banks and creditors: How does my organization reflect adequate vendor oversight to federal regulators?

As mentioned earlier, vendor management is not a new concept to your organization and as a result the ability to leverage exists. Documenting vendor oversight should be handled via a multifaceted approach. In most cases, the vendors related to your identity theft prevention program are classified as critical service providers because they handle nonpublic customer information. The program administrator should ensure that the organization’s vendor management program properly captures the service provider. This will include verifying that due diligence and ongoing monitoring procedures address identity theft risk. Once validated, your program can simply reference the reliance on the institution’s overall vendor management program. The program administrator should then place a formal request to the vendor for a red-flag clause in the service agreement. As discussed previously, this request will likely be denied. At this point the program administrator should highlight the controls and systems the service provider has in place to protect customer information. This can be achieved through the reference of SAS 70 reports and existing contract clauses concerning the protection of customer data. Your objective is to demonstrate to regulators that while your company does not have a formal red-flag contract clause, the service provider has effective policies and procedures in place to protect customer data and inform its customers of any breaches that may compromise that protection. Lastly, the program administrator should document that the vendor’s contract is not to be renewed unless a red-flag clause or similar contract addenda is injected into the service agreement. This can be achieved by documenting these criteria in the vendor management program or by issuing a formal memo to the individual who manages vendor contracts at your organization.

Examination Preparation

It is a natural reaction for compliance and risk officers to, after a federal rule is finalized, identify the regulatory expectations. A compliance officer’s mind will race with a variety of questions: How often should we update our program? How should we document our analysis? What should our program look like? Without fail, many examiners will provide one of two tried and true responses—“I’ll know it when I see it” or “it depends”—two staples in the unofficial

A compliance officer’s mind will race with a variety of questions: How often should we update our program? How should we document our analysis? What should our program look like?

Illustration A

	FCRA RULE DESCRIPTION	EXAMINATION PROCEDURE REFERENCE
OCC	Affiliate Marketing & Opt-Out Notices	Bulletin 2008-28 —FCRA Examination Procedures, Module 2
	Duties Regarding Notices of Address Discrepancies	Bulletin 2008-28 —FCRA Examination Procedures, Module 4
	Detection, Prevention, & Mitigation of Identity Theft	Bulletin 2008-28 —FCRA Examination Procedures, Module 5
	Duties Regarding Changes of Address	Bulletin 2008-28 —FCRA Examination Procedures, Module 5
OTS	Detection, Prevention, & Mitigation of Identity Theft	Bulletin RB 37-27 —Examination Handbook, Section 341*
	Detection, Prevention, & Mitigation of Identity Theft	Bulletin RB 37-27 —Examination Handbook, Section 1300, Module 5
	Duties Regarding Notices of Address Discrepancies	Bulletin RB 37-27 —Examination Handbook, Section 1300, Module 5
	Duties Regarding Changes of Address	Bulletin RB 37-27 —Examination Handbook, Section, 1300, Module 5
FDIC	Detection, Prevention, & Mitigation of Identity Theft	FIL-105-2008 —Examination Procedures, Identity Theft Red Flag Section
	Duties Regarding Notices of Address Discrepancies	FIL-105-2008 —Examination Procedures, Change of Address Section
	Duties Regarding Changes of Address	FIL-105-2008 —Examination Procedures, Address discrepancy Section

*The OTS revised Examination Handbook Section 341, Information Technology Risks and Controls, to include guidance on the Identity Theft Red Flags as part of the Information Security guidance.

**Review to be performed by Risk Management Examiners.

examiner handbook. (I speak from experience, as I was privy to the conceptual handbook at one point during my career.) In this scenario, however, regulators were truly placed in a challenging position when charged with developing examination procedures. As a result, the examination procedures released by federal regulators are rather broad and will likely be enhanced (or complemented with Q & A guidance) as the industry defines the features of an acceptable identity theft prevention program. Many organizations will undergo review prior to the release of any additional regulatory commentary. This leaves administrators with a critical question: How should I prepare for my examination?

Preparation for an examination must start with review of your governing examination procedures. As seen in Illustration A, the exam procedures utilized during your organization's review may vary between federal regulators. In fact, the procedures released by the FDIC, OTS, and OCC all differ. It is possible that various examiner divisions will participate in the review of your FCRA compliance, and that the reviews occur years apart. This "silo" review approach could complicate the exam process for your institution. Despite these anticipated complications, this information can be valuable to the administrator during examination preparation. For example, the FDIC has stated that its risk

management examiners will be assessing compliance for 12 CFR Section 334.90.⁴ If you are an FDIC bank, it is likely that risk management (or IT specialized) examiners have previously reviewed your GLBA and information security risk assessments. When assembling the structure of the program's risk assessment, one should incorporate the components of those established assessments that have received positive examiner feedback in the past. This basic approach allows an institution to leverage existing resources while also presenting information to examiners in a familiar format.

Another area where the administrator can alleviate confusion for examiners resides in the manner in which your program is presented. Commentary within the initial release of the final rules provides insight regarding the envisioned design of a program. Again and again banks have been encouraged to leverage existing procedures and not to develop separate duplicate documentation. Leveraging can save valuable time for banks, but can also complicate the review for an examiner. To ensure a smooth review, the administrator should assemble a master copy of the program that includes all referenced policies, procedures, and forms. This will serve two purposes: First, the copy will allow the administrator to centrally manage the information that is being presented to examiners and auditors. Recall that the review of the new

Illustration B SAMPLE DATABASE TABLE

Last Name	Date Reported	Amount	Date of Birth	Age	Age Bracket	Access Device Utilized	Compromised Account	Business Line
Name 1	3/1/2009	\$200.04	6/15/1960	48	40–49	Debit Card	Product 357	Retail Banking
Name 2	3/15/2009	\$ 40.20	8/2/1974	34	30–39	Debit Card	Product 159	Call Center

FCRA rules may adopt a silo approach. A master program copy (including all referenced resources) will enable easier management of this examination approach. Second, and more importantly, the creation of a master program copy will force the administrator to reconcile all referenced resources. It is not uncommon for a bank to have empty references within its program. For example, a program may refer to the organization’s vendor management program within the section that discusses oversight of service provider arrangements. However, review of the vendor management

program may reveal that the reference was never incorporated as intended. This aggregate reconciliation could also uncover forms that require updating or other items that were overlooked during the program’s development. While simple in nature, these measures can make the difference in ensuring a successful examination.

The Reflection Pool

Those who have attended seminars covering the topics of fair lending practices or the Home Mortgage Disclosure Act (HMDA) have probably heard the continuously regurgitated concept of knowing your HMDA data

(See related article on page 22.). The concept focuses around an organization’s ability to collect data, perform peer analysis, and adjust policies and procedures to enhance its program. While the concept is discussed at great length in the arena of fair lending, a financial institution must adopt a similar methodology to effectively manage its identity theft prevention program. One of the required program elements set forth by Section 334.90 is to “ensure the program is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.”

Appendix J goes further, stating that in order to properly update a program an institution should consider “the experiences of the financial institution or creditor with identity theft.” Management of your organization’s past experiences with identity theft is arguably the most important part of the identity theft prevention program.

Each organization should maintain a centralized past experiences log. In order to support a log of this nature, the bank or creditor must have a system in place to forward all identity theft cases from each business line to a centralized location. Given the broad definition of identity theft, the manner in which these cases are filtered will vary depending on the size and complexity of your institution. It may take your organization several months to calibrate the acceptable amount of information that is forwarded to the administrator or team that manages the program. During the input phase, there should be several classifications assigned to each case. For example, recommended classifications include the victim’s age, date reported, reporting business line, affected account type, and compromised access device. Illustration B displays a sample database table that can be implemented. The assigned classifications enable an organization to perform a detailed analysis of its experiences. Using such a table, the company can develop metrics that indicate information such as the average age of its customers who are identity theft victims, the fiscal quarter that experiences the most identity theft cases, average and median amounts of losses, and various other data that is pertinent to the risk management process.

After a comprehensive past experiences log and metric deck have been developed, the administrator should ensure the information is being utilized effectively. Many of these exercises can be documented as evidence that your program is periodically updated as required by the regulation. A basic of use of your log will be to identify business lines, account types, and customers that appear to have increased identity theft risk exposure.

Another basic use for the past experiences log is to compare your institution’s experiences to community data in order to identify anomalies. This can easily be done by referencing complaint data published by the FTC in its annual *Consumer Fraud and Identity Theft Complaint Data Report*. This comparison can show whether your program should implement enhanced controls in specific geographic footprints or if your bank has experienced a high volume of a particular type of fraud.

The administrator should also ensure metric decks are leveraged throughout your organization. The data could have a variety of uses to business lines such as assisting the marketing department in creating ads or alerting a loss prevention team to evolving fraud trends affecting the company.

Many organizations will undergo review prior to the release of any additional regulatory commentary. This leaves administrators with a critical question: How should I prepare for my examination?

One of the most important uses of the past experiences log is to provide justification. Section 334.90⁵ requires that a program “be appropriate to the size [and] complexity of the financial institution or creditor and the nature and scope of its activities.” By having a strong grasp of the identity theft experiences that directly effect your institution and your service footprint, the administrator will be able to substantiate the structure of the program. Using comprehensive metrics can support a strategic program decision to exempt an account type that is not automatically deemed a “covered account” by the regulation. The past experience data can also validate the investment in automated systems to executive management or a board of directors.

Similar to most federal requirements, there is not a silver bullet an institution can implement to ensure compliance. The FCRA rules do not lay contest to that belief. However, a company can take large strides toward effectively managing an identity theft prevention program by taking the necessary measures to address these industry challenges. **BC**

ABOUT THE AUTHOR

John P. Bonora, CRCM, is currently a vice president and compliance officer for Fairfield County Bank, headquartered in Ridgefield, Conn. Prior to joining FCB, he served as an audit supervisor for Webster Bank, N.A., where he specialized in regulatory compliance internal auditing. Mr. Bonora has also served as a consultant/auditor to more than 40 financial institutions based

in New England. During 2008 he founded Privacy Solution Partners, LLC, a private consulting company specializing in identity theft education and prevention services for consumers. Before entering the private sector, he was a senior bank examiner for the Commonwealth of Massachusetts Division of Banks. Mr. Bonora earned a bachelor’s degree in economics/finance from Bentley College and has completed the FDIC’s Division of Supervision and Consumer Protection Risk Management Training Program. He is also a Certified Regulatory Compliance Manager with the American Bankers Association’s Institute of Certified Bankers. Mr. Bonora publishes a free quarterly electronic newsletter, The Identity Guard, which focuses on providing identity theft prevention information to consumers. Reach him by e-mail at john.bonora@fairfieldcountybank.com or john@privacysolutionpartners.com, or visit www.privacysolutionpartners.com.

Endnotes

- ¹12 CFR §334.90 (e) (4).
- ²12 CFR §334.90 Appendix J (VI) (c) Oversight of Service Provider Arrangements.
- ³FFIEC Interagency Guidelines Establishing Information Security Standards—VII. Overseeing Service Providers: Contracts with Service Providers.
- ⁴12 CFR §334.90 Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft.
- ⁵12 CFR §334.90 (d)(1).

Paying too much for CRA, HMDA or Fair Lending solutions?

We have delivered “Peace of Mind” for over 20 years.

Consulting - Let our experts provide you with guidance.

CenTrax Software - Easy, Complete, Affordable...really!

Services - We can do this work for you. You deserve it.

MARQUISTM

800.365.4274

GoMarquis.com

Reach this advertiser through <http://links.aba.com>

