

# Information Security and Privacy Liability Exposures and Risk Management

By Mark Greisiger, President, NetDiligence  
David Navetta, Esq., President, InfoSecCompliance, LLC



610.658.0913

[mark.greisiger@netdiligence.com](mailto:mark.greisiger@netdiligence.com)

Philadelphia Office  
P.O. Box 204  
Gladwyne, PA 19035  
[www.netdiligence.com](http://www.netdiligence.com)

*e-Risk should be a choice, not a fate...*

## InfoSecCompliance LLC

*A Law Firm Providing Information Security and Privacy  
Contracting, Legal Compliance and Insurance and Risk Management Consulting*

303.325.3528

[djn@davidnavetta.com](mailto:djn@davidnavetta.com)

Denver Office  
3379 W. 35<sup>th</sup> Ave  
Denver, CO 80211

## INTRODUCTION\*

Whether a financial institution has an Internet presence or merely utilizes its own internal networks, customer privacy and protecting customer data from loss or theft are major business issues impacting all financial institutions (FIs). Since all FI's rely on computers and information to do business, and based on the risks posed by the current legal environment, FIs of all sizes and types must address security and privacy risk.

At stake is customer trust, a solid compliance standing with regulators, and avoiding costly class action liability lawsuits due to a breach. Since "breach notice laws" are effective in over 37 States, FIs are now required to report security incidents, and *reasonably suspected* security incidents, which involve customer personally identifiable information. As a result of these breach notice laws a 'ripple effect' can occur, starting with the FI's breach being published as a headline news story. This negative publicity can impact consumer relationships, undermine marketing expenditures and cause serious harm to a FI's reputation and revenue streams. The ripple effect caused by the legally mandated notice can also invite regulatory scrutiny under Gramm-Leach-Bliley Act (GLB) and lead to the payment of damages and attorneys fees to defend lawsuits.

It is no secret that information technology has enhanced the capacity of most FIs to collect, store, transfer and analyze vast amounts of data about consumers. One can hardly visit a FI website today without various customer-facing e-banking features. This, along with the myriad subsequent uses of this personal information and highly publicized stories concerning identity theft, has raised public awareness and consumer concerns about online security and privacy.

To address these concerns, most FIs have formal privacy and security programs and policies in place. However, the issue of complying with such policies is not always clear-cut. FIs must work hard to align their online *and* offline banking and business practices with these policies. Although the Internet web environment is where many of the security/privacy violations occur, customer information is more commonly exposed by employee carelessness (such as bringing a laptop home with unencrypted customer information), software glitches and "inside jobs" by bank employees with authorized access to such information.

Relationships with service providers and partners are another area of security and privacy concern. The second a FI provides sensitive information to a service provider or partner, the strengths of the FI's internal controls become irrelevant and the FI is completely reliant on the service provider's security and privacy practices. This is why laws like GLB and contractual requirements such as Payment Card Industry Data Security Standard require FIs to conduct security assessments and contractually impose duties on service providers to maintain adequate security controls. Moreover, contractual security incident reporting terms are necessary to address breach notice laws.

To address these risks, FIs must engage in a comprehensive risk management program that typically includes security and privacy assessment, legal compliance and contracting review and risk transfer through insurance. Security policies and procedures should be assessed for adequacy and regulatory compliance by information security professionals and attorneys with knowledge of these issues. Security and privacy compliance assessments should be performed to ensure that a FI is actually complying with its own policies and procedures. Attorneys should work with security professionals and business interests to analyze legal compliance and draft and negotiate contract language that addresses security and privacy controls. When a FI uses a service provider or intends to provide sensitive customer information to a third party for any reason, contract language should be put in place that requires such entities to maintain compliant security and privacy practices.

## Privacy Management

To better manage and mitigate security and privacy-related risk, corporate risk managers, legal counsel, privacy managers and compliance officers should, as a baseline measure, implement in good faith all the requirements of GLB Section 501b for security. However, security is only one aspect of privacy risk. Security deals with a company *protecting* personally identifiable information from "bad actors" intent on stealing such information. In addition to protecting personally identifiable information, privacy management also involves an organization's handling of such information, including the collection, transfer/sale and integrity of such information.

In general, FIs should endeavor to create privacy policy/ programs that are consistent with the Fair Information Practice Principles (FIPP), which include:

- *Notice and Awareness*
- *Choice and Consent*
- *Individual Participation and Access*
- *Security, Information Quality and Integrity*
- *Enforcement, Accountability and Recourse*

(these principles are often abbreviated and referred to as Notice, Choice, Access, Security and Enforcement). Originally established by the Federal government in the 1970s, the five principles form the basis of most privacy legislation now being enacted. They are also widely adopted by self-regulatory bodies such as the Online Privacy Alliance (OPA). Since modern privacy laws are based on these principles, most organizations developing privacy programs build their policies and procedures around FIPP.



**Notice.** Notice is the mechanism that a FI uses to advise its customers of its privacy practices. In general, such notice is contained in the FI's privacy policy and describes the collection and use practices concerning personally identifiable information (data used to identify, contact, or locate a person). The privacy policy is communicated by sending it to the customer or posting it on the FI's web site. Specifically, a privacy notice should inform consumers of:

- the purposes for which the FI collects and uses information about its customers;
- the types of technologies used on the website to 'personalize' or track the customer's visits (i.e. online application forms, cookies, etc.)
- how to contact the FI with any inquiries or complaints;
- the names or types of affiliated and third party companies to which the organization discloses the information it collects; and
- the choices and the means customers have for limiting use and disclosure of their data.

**Choice.** Choice gives customers options over how their personal information can be collected, used and/or shared. Among other items, the choice component typically addresses consumers' ability to:

- 'opt in' or 'opt-out' of the FI's marketing campaigns;
- restrict the sharing of their personal information with affiliates and third parties for marketing purposes;
- control the communications channels (e.g. mail, email, phone, etc.) for marketing and the frequency of communications; and
- opt-in or out of the sharing of sensitive information.

The choices listed above are not necessarily mandated by specific legislation, but should be considered in the context of enhancing customer trust.

**Access.** A FI should give customers reasonable access to the information collected about them. Reasonable access may be provided, for example, by giving individuals an easily understandable copy of the information held about them. Access is also the key to allow customers the opportunity to correct, amend or delete inaccurate information.

**Security.** Paramount to a privacy program is the security of customer data, which protects the confidentiality, integrity and availability of such data. In a digital economy it is difficult to maintain an acceptable level of privacy standards without strong network security practices. This includes having essential [baseline] controls in place to safeguard personally identifiable information (PII). While the adequate mix of controls can vary, some control examples include use of ‘2-factor’ authentication technology for system access, ‘hardened’ public-facing systems with a firewall and an intrusion detection system, and encryption technology when transmitting and storing sensitive customer information. At every step in a FI’s handling of data, the FI should see that data are carefully *stored, transmitted, processed and protected*. FIs should have procedures to ensure that data are reliable for its intended use, and that it is accurate, complete and current. Moreover, all service provider contracts involving the exchange of consumer information should have security and privacy clauses that document how these requirements will be met.

**Enforcement.** Enforcement should include the ability to measure compliance with security and privacy programs and meaningful sanctions for privacy abuses and lack of compliance. A FI’s security and privacy policy is just words until actions are taken to implement it. Although often called “self-regulatory measures,” many industry-developed measures rely heavily upon enforcement by consumer protection agencies, such as the OCC or Federal Trade Commission. Crucial to the enforcement component are mechanisms for ensuring compliance with the stated privacy policy and principles, recourse for individuals whose data may have been misused and consequences to a person or organization for non-compliance. Such mechanisms can include:

- an independent recourse procedure for complaints that includes damage awards;
- a procedure for the verification of statements financial institutions make about their privacy practices; and
- an agreement to remedy problems related to these principles, and to hold offending individuals or companies accountable for non-compliance.

## Security/ Privacy Regulatory and Legal Liability

**Summary of Security and Privacy Legal Liability Risks.** Now more than ever companies, including FIs, face a wide range of privacy and security liability risks. The scope of this risk has expanded significantly over the last decade for two reasons. First, is modern business’ almost complete reliance on information technology and/or the Internet to do business. Second, is the existence of a patchwork of local, State, Federal and international laws that regulate privacy and security. The Internet expanded the scope of operations for most companies, and it is possible, for example, for a company to have a database of customers that is subject to the laws of all 50 States. Thus, even smaller organizations with national or international reach may need to worry about dozens of privacy and security laws. The following table outlines the various security and privacy risks an organization may face in the normal course of business:

Privacy Risk Description	Example
<b>“Traditional” Media Privacy Risks Modernized</b>	
Intrusion upon seclusion using communication devices	<ul style="list-style-type: none"> <li>▪ Intrusion upon seclusion morphed into electronic realm, including for example, fax-blasting, telemarketing, spam, cookies and spyware</li> </ul>
<b>Protection Privacy Risks: risks concerning protection of PII from unauthorized persons</b>	
Protection Risks (Information security): failure to protect private information from theft by others or disclosure to unauthorized persons	<ul style="list-style-type: none"> <li>▪ Insider job at Bank of American and Wachovia lead to the exposure of the account information of 676,000 customers</li> <li>▪ 1.2 million customers had bank account information potentially exposed when Bank of America lost a back-up tape in route to storage</li> </ul>

Privacy Risk Description	Example
<b>Protection Privacy Risks (cont.): risks concerning protection of PII from unauthorized persons</b>	
<b>Failure to Warn Risks:</b> failure to warn of actual or suspected unauthorized access to PII (e.g. breach notice laws)	<ul style="list-style-type: none"> <li>A company believes that its customers' personal information was compromised, but fails to warn its customers so they can take action to protect their credit (in violation of breach notice laws)</li> </ul>
<b>Information Handling Risks: risks concerning collection and handling of PII</b>	
<b>Collection Risk:</b> intrusively or secretly collecting PII without the consent of the individual	<ul style="list-style-type: none"> <li>Cookies, spam, pop-up ads, spyware, telephone marketing that collects information, including collection without knowledge of individual; pre-texting (i.e. social engineering)</li> </ul>
<b>Handling Risk:</b> mishandling of PII, disclosing PII in a fraudulent manner or providing PII to bad actors without consent	<ul style="list-style-type: none"> <li>Unauthorized sale or transfer of PII to a service provider, telemarketer or partner without consent of the consumer or the proper contractual requirements in place</li> </ul>
<b>Choice/Consent Risks:</b> failure to provide person with choice on how their PII is collected/handled, including failure to provide opt-in/opt-out	<ul style="list-style-type: none"> <li>Failing to provide an opt-out functionality for mass commercial e-mails (e.g. CAN-SPAM)</li> <li>Failure to obtain consent to provide information to non-affiliated third parties under GLB</li> <li>Failure by a bank to allow opt-out of marketing offers from affiliate sharing as required under Fair and Accurate Credit Transactions Act</li> <li>Failure by a bank to allow opt-out of affiliate information sharing under the Fair Credit Reporting Act</li> </ul>
<b>Notice Risks:</b> failure to provide notice of PII handling practices or the provision of inadequate or fraudulent notice	<ul style="list-style-type: none"> <li>Under GLB, financial institutions must provide notice to their customers prior to providing personal financial information to any nonaffiliated third party</li> </ul>
<b>Accuracy/Integrity Risks:</b> disseminating inaccurate PII or failure to correct PII	<ul style="list-style-type: none"> <li>Under FACTA, consumers have a right to directly dispute the accuracy of credit information with a FI that furnished it, and the FI must investigate and not report negative information while the investigation is pending</li> </ul>
<b>Access Risks:</b> failure to provide access to collected PII	<ul style="list-style-type: none"> <li>Under HIPAA, individuals are afforded a right access their personal health information</li> </ul>
<b>Inadequate Privacy Policy: privacy policy does not exist or contain certain provisions required by law or is unfair or deceptive to consumers</b>	
<b>Lack of Privacy Policy:</b> failure to have a privacy policy	<ul style="list-style-type: none"> <li>California law that requires a privacy policy for companies collecting personal information from California residents</li> </ul>
<b>Inadequate Privacy Policy:</b> missing or inadequate privacy policy provisions	<ul style="list-style-type: none"> <li>A privacy policy that is ambiguous as to how a consumer is to consent to having their information shared with third parties</li> <li>A privacy policy that is changed from a prior privacy policy that provided more protection</li> </ul>

The following chart outlines some of the statutes and regulations addressing the various privacy risks outlined above:

Privacy Protection Laws	
Privacy Risk Addressed by Law	Examples of Laws Addressing Privacy Risk
Privacy Protection (information security) Laws	Gramm-Leach Bliley (GLB --Financial Industry); Section 5 of the Federal Trade Commission Act; and California AB 1950
Failure to Warn Laws	California SB 1386 and “Breach-Notice Laws” in 37 States
Intrusion upon seclusion	Junk Fax Prevention Act of 2005 (JFPA); Telephone Consumer Protection Act of 1991 (TCPA); and Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
Information Handling & Privacy Policy Laws	
Name and Description of Law	Areas Regulated
<b>Gramm-Leach Bliley (GLB - Financial Industry):</b> comprehensive privacy law regulating financial institutions (banks, insurance companies, brokers, etc.)	PII Collection; PII Handling; Choice/Consent, Notice and Privacy Policy requirements
<b>Fair Credit Reporting Act (Consumer Credit Agencies):</b> law regulating the collection, handling and accuracy of private consumer credit information	PII Collection, PII Handling, Accuracy/Integrity, Access Laws
<b>Electronic Communications Privacy Act (aka Stored Communications Act):</b> regulates the unauthorized access (e.g. wiretapping) and disclosure of in transit and stored electronic communications	PII Collection and PII Handling Laws
<b>Fair and Accurate Credit Transactions Act:</b> appended to FCRA for purposes of addressing identify theft	PII Handling (disposal of credit reports), Accuracy/Integrity (disputed credit information); Choice/Consent

### **Negligence and Class Action Lawsuits**

In addition to specific regulations and statutes, common law negligence may also become problematic for FIs. Currently, while the plaintiffs’ bar has brought several class action lawsuits against organizations for security breaches that exposed personally identifiable information, there has not been a significant “break-through” case that has gone beyond a motion to dismiss or achieved the certification of a class action. To date, for security breach and identify theft cases, the plaintiffs have been unable to establish the “damages” requirement for negligence. In essence, courts have ruled that a consumer taking pre-emptive actions to protect his or her credit has not suffered compensatory damages. Moreover, even if a consumer can show that they suffered identity theft they still have to establish that the security breach was the cause of such identity theft (in theory the consumer’s personal information could have been obtained from a multitude of sources). Nonetheless, FIs still face the prospect of expensive attorney fees to defend these actions, and if the plaintiffs’ bar breaks through they could face significant liability.

### **Key Areas of Liability Concern for Financial Institutions**

While there are a myriad of privacy and security laws on the local, State and Federal level, there are some key concerns that FI should address. This list is by no means exclusive and FIs should seek to achieve compliance with every privacy and security law that applies to them. This requires the legal assistance to determine the laws that apply to a FI and the most cost-effective way to work toward compliance.

## Gramm-Leach-Bliley Act

GLB is a comprehensive privacy and security law that FIs must adhere to. GLB covers both information handling practices and security practices for “nonpublic personal information” (NPI). On the information handling side, FIs must create privacy policies that set forth their information handling practices, provide adequate notice and present opt-out opportunities for sharing of NPI. GLB also constrains the sharing of NPI to nonaffiliated third parties by requiring contracts that limit the use of NPI by such third parties. FIs should review their privacy policies and NPI-sharing practices and work toward complying with GLB’s information handling practices.

In addition, FIs must work toward complying with GLB’s security requirements. The drafters of the GLB SafeGuards Rule, while requiring a comprehensive security program, also intended to infuse some flexibility into the GLB security requirements:

You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards *that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue* (emphasis added).

In addition to a comprehensive security program to address a FI’s internal security environment, GLB also requires FIs to conduct a due diligence in the selection of service providers handling NPI and to contractually impose the GLB security requirements on those service providers:

You shall:

1. Exercise appropriate due diligence in selecting your service providers;
2. Require your service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and
3. Where indicated by your risk assessment, monitor your service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, you should review audits, summaries of test results, or other equivalent evaluations of your service providers.

(From the FFIEC’s **Interagency Guidelines Establishing Standards for Safeguarding Customer Information**, the entity charged with establishing GLB implementing rules for banking entities).

In short, FIs have a significant challenge addressing both GLB’s internal security requirements as well as their “external” security environment with respect to service providers handling NPI. One of the main difficulties in addressing GLB is the multi-disciplinary approach that is required - FIs need to involve security professionals, risk managers and attorneys to put proper security and privacy programs into place. This especially true on the contractual front when dealing with service providers. FIs should work with security professionals to assess their service provider’s information security as well as attorneys to draft terms requiring compliance with GLB’s security and privacy requirements.

## Privacy Policies - Matching Policies with Practices

One of the most significant areas of legal and regulatory risk is the matching of the practices set forth in a privacy policy with the *actual* practices of an organization. While privacy policies are generally not considered “contracts” per se, FIs can get into trouble when they “over-promise” or ignore their own privacy policy. In fact, this is one of the areas that Federal (e.g. the FTC) and State regulators have been most active. These types of actions are usually couched in terms of “consumer fraud” or “deceptive trade practices,” which allow regulators to pursue organizations under general consumer protection statutes. The problem can be especially acute for FIs with decentralized units or subsidiaries and multiple privacy policies - where it is possible for one unit to make certain promises concerning personal information handling while another unit is unaware of those promises and undertakes prohibited actions. Again, FIs must engage in a coordinated effort (involving privacy personnel and attorneys) to understand exactly what privacy policy representations they are making publicly, educate the employees of the FI and work to match privacy policy representations with the FI’s actual practices.

## Breach Notice Laws

Breach notice laws have been passed in 37 States and additional bills are pending in several additional States. These laws vary from State to State, but generally require organizations that hold personally identifiable information of customers to report actual or reasonably suspected security breaches that have exposed such information. FIs, often holding thousands if not millions of personal information records, can be subject to expensive legal and notification costs in the wake of a security breach. There are several issues that make breach notice laws a difficult problem.

First, the laws are typically tied to the citizenship of the individuals whose information was exposed. Therefore, a FI handling a database with customers from all 50 States must comply with the breach notice laws of all 37 States that are currently in place. While the thrust of each of the laws is similar, they do vary in some key aspects such as the type of notice required and most importantly the “trigger” for providing notice. For example, each of these four States has a substantively different notice trigger:

- **Arizona:** “personal information was or is reasonably believed to have been acquired by an unauthorized person”
- **Colorado:** “the likelihood that unencrypted personal information has been or will be misused”
- **Connecticut:** “personal information was or is reasonably believed to have been accessed by an unauthorized person”
- **Florida:** “Notice is not required if after reasonable investigation the person determines there is no reasonable likelihood of harm to customers.”

Therefore, for a security breach involving a database containing an Arizona and Colorado resident, there may be a duty to report in Arizona because all it requires is acquisition by an unauthorized person, while in Colorado the FI may be able to reasonably conclude that despite the breach there is not a “likelihood [of] misuse.” Attorneys must work with the FI’s risk managers and security professionals to make this determination. However, it may come down to the State with the least rigorous reporting requirement, and that would necessarily trigger notice to all potentially affected customers.

Second, most of the breach notice laws provide a “safe harbor” for personally identifiable information that is encrypted. The breach notice laws basically do not require notice of the breach when the personal information has been encrypted. Unfortunately, encryption in storage and in transit is not always easy or inexpensive for an organization to implement. This is another area where information security professionals should be consulted to determine feasibility and costs - for some organizations, because of the consequences that can arise out of breach reporting (discussed below), it may be worth the up-front investment in encryption technology.

Third, FIs can face duties and potential liability under breach notice laws if their service providers suffer a security breach exposing the personally identifiable information of the FI’s customers. Practically speaking, complying with breach notice laws requires carefully selecting service providers that have good security, and most importantly imposing contractual duties on such service providers to provide notice to the FI in the event the service provider suffers (or reasonably suspects) a security breach exposing customer information.

Last, if a duty is triggered under a breach notice law, FIs must consider the consequences beyond the expenses of analyzing the law and providing notice. One of the first consequences of the notice is damage to the FIs reputation, stock price and/or customer base. Prior to providing notice FIs should have a crisis management and public relations plan in place to mitigate these types of “intangible” losses. Moreover, more and more often, organizations are getting hit with class action lawsuits by consumers and lawsuits by “issuing banks” after a breach. Notice can also lead to regulatory scrutiny, especially if it appears that the FI was not compliant with industry laws such as GLB or if they “over-promised” concerning their security practices in their privacy policy.

## Merchants and Service Providers

As set forth above, under GLB and with respect to breach notice laws, FIs should conduct due diligence assessments of their service providers and impose contractual duties to maintain adequate security and report security breaches. However, there is another potential source of liability for some FIs that are involved with the credit card payment system.

Banks acting as “merchant banks” or “acquiring banks” can also face legal liability if the merchants they serve suffer a security breach. The major credit card associations contractually require merchant banks to work with merchants that comply with the Payment Card Industry Data Security Standard (“PCI Standard”). For acquiring banks utilizing the credit card payment system, if one of their merchants suffers a security breach exposing credit card information, the acquiring bank may be fined up to \$500,000 by a credit card association if the merchant did not satisfy the PCI Standard. In addition, the acquiring bank may be sued by “issuing banks” that are required to reissue credit cards.

This has already happened in cases of security breaches involving B.J. Wholesalers and TJX Companies (e.g. parent company of T.J. Maxx). In the TJX matter, one bank has sued TJX and claimed that the cost of re-issuing a credit card is \$20 per card. Unfortunately, it appears that TJX may have allowed 45 million credit card account numbers to be exposed (however, thus far it appears that only one bank has sued TJX). ***Significantly, Fifth Third Bank was named as co-defendant in its capacity as TJX’s acquiring bank or credit card processor.***

Similar to the requirements under GLB and breach notice laws, the main way for acquiring banks to deal with this type of risk is to conduct security assessments based on the PCI Standard and impose security contract terms requiring merchants and service providers to comply. In fact, Section 12.8 of the PCI Standard explicitly mandates that merchant banks and merchants contractually require service provider to adhere to the PCI Standard. The process of creating contract terms around security requires cooperation between security professionals and attorneys. The security professionals must assess the providers and make sure that the contract language substantively addresses any security issues or weaknesses. The attorneys must “translate” the substantive security concerns into contract language that is legally binding and effective. This process can be difficult since both the attorney and security professional typically do not fully understand each others’ worlds. One solution is to create security schedules that can be attached to the FI’s contracts, and modified to meet particular needs and circumstances. Security language should include terms related to maintaining security controls, security breach response, monitoring and enforcement of duties and transfer of risk of loss.

## Solutions - What Can be Done?

So, what do FIs do to make their offline business practices and website practices match their stated privacy policies and comply with applicable regulations? What do FIs need to do in order to manage their service provider and merchant relationships? How can residual security and privacy risk be dealt with? There are no simple solutions to these problems, but there are some key areas that FIs should address:

- (1) **Security and Privacy Assessment** - Work with security and privacy professionals to assess the FI’s security and privacy policies and practices to determine whether they meet industry standards and legal compliance standards, and to determine whether stated privacy and security policies are being followed in reality;
- (2) **Legal Review and Contract Drafting** - FIs must have attorneys work with security professionals to determine the applicability of security and privacy laws, interpret applicable laws and put policies and procedures in place that comply with those laws. Attorneys are also key for addressing external contractual relationships with service providers, including drafting privacy and security contract terms as required under law and to establish security controls, incident response, enforcement and monitoring and transferring risk of loss; and
- (3) **Security and Privacy Insurance** -- No matter what measures a FI takes or how much it spends on security or attorneys, residual risk will always exist. FIs may transfer some of this risk to service providers through contractual risk transfer terms, but some will still remain. There are several insurance companies that offer policies that cover security and privacy liability risks. In terms of cost/benefit analysis, FIs could conceivably spend large amounts of money to become as safe as Fort Knox, but that would not make sense from a business perspective. Insurance can ultimately save an organization money by allowing it to spend what it needs on reasonable security (not perfect security) and have risk transfer mechanism to look to when an unexpected event occurs.

### ***Security and Privacy Assessment -- GLBA 501b Security Review***

FIs must consistently assess their security and privacy practices and compare them against the mandates within regulatory requirements. They should also benchmark themselves against their peers (such as other FI's of similar asset size) to address "industry standards." Financial institutions should inspect their business practices, network operations and their Internet banking websites to verify that the functional implementation complies with their stated privacy and security policy, especially when it is posted on their website. After any review, the organization will need to implement recommended changes and put processes in place to ensure that it will continue to assess its ever-changing sites and business practices on an ongoing basis.

FIs need to continually analyze the effectiveness of their cybersecurity controls and processes in order to establish due care and a defensible security and privacy program. As part of the review, FIs need to identify security gaps or weaknesses in their business practices. The goal is to understand how current legislation impacts their financial institution operations, and then strive to define a good faith path for achieving a level of compliance, while also mitigating potential liability due to known deficiencies. Any network risk security assessments implemented should also serve to help the organization improve their overall privacy and security posture in tandem. This might include assessing the following items:

- FI objectives for collecting, managing and using personal information;
- adherence to known security standards, such as ISO 17799. This can help assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks;
- identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
- assess the likelihood and potential impact of these threats, taking into consideration the sensitivity of customer information; and
- insurance clauses requiring service providers to purchase insurance covering security and privacy risks.

### ***Legal Review and Contract Drafting - Development of Information Security and Privacy Contract Schedules***

To efficiently handle security issues surrounding FI's use of service providers, FIs should develop a security and privacy contract schedule that can be appended to service provider contracts. The purpose of such contract language is to require service providers to match the FI's internal security and privacy risk tolerance. As such, the contract schedule should include:

- "preventative" contract terms that mandate security and privacy controls in order to prevent a security incident and comply with regulatory requirements (including those under GLB);
- compliance and enforcement contract terms that provide the FI with the right to check if its service providers are complying with the schedule;
- security incident contract terms to set forth the service provider's notice and remedial duties in the event it suffers a security breach; and
- risk of loss contract terms that allocate who is responsible for absorbing loss if the service provider suffers a security breach.

To create efficiencies and manage the flow and expectations of the service provider contract negotiation process, FIs should put a formal written process in place for implementing and negotiating security and privacy contract terms. That process should include:

- a risk assessment of the service provider's controls (as required under GLB);
- the addition of contract language that addresses the specific risks of the transaction beyond what is contained in the basic security and privacy schedule (if necessary); and
- a vendor management program by which the FI periodically confirms that its service provider is doing what it promised to do in terms of security.

By establishing a comprehensive vendor management process, Vendors will be in a stronger position to monitor and manage their service provider security and privacy risks.

## **Security and Privacy Insurance - Analysis of Available Security and Privacy Insurance**

Despite a FI's best efforts, and regardless of the amount of resources expended on security and privacy controls, there is no such thing as "perfect security." There is always a level of risk that is tolerated or retained by a FI internally and with respect to using service providers. This is where security and privacy insurance comes into play. Companies can transfer residual security and privacy risk to insurance companies.

Security and privacy insurance now exists to cover liability arising out of security breaches or negligent privacy practices (e.g. collection and transfer of personal information). Moreover, coverage exists for "1<sup>st</sup> party" losses caused by security breaches, including income loss, extra expense, restoration of corrupted digital assets, crisis management and public relations expenses and extortion payments. Of significance, FIs can now purchase insurance that covers the costs associated with providing notice to FI customers in accordance with breach notice laws when their personal information has been exposed. When dealing with service providers, FIs can contractually require them to carry security and privacy liability insurance and naming the FI as an additional insured.

The key to using insurance as a risk management tool is understanding the risks a FI faces (through a security and privacy assessment), and determining whether the FIs existing insurance policies, and/or other insurance policies available on the market, will cover any of the risks the FI does not want to retain. Fortunately for FIs, now more than ever there are insurance solutions that address security and privacy risks. Unfortunately, however, the large number of options and varying approaches can be confusing. Care should be taken in identifying the security and privacy risks a FI wants to transfer, and ensuring that such risks are actually transferred to the insurance company based on the wording of the policies at issue. The goal is to avoid costly "coverage gaps."

### **Concluding Remarks**

Security risk exposures and prudent privacy management practices should be factored into corporate enterprise risk management programs. For the best protection, a comprehensive security and privacy program should be implemented that includes risk assessment, service provider security and privacy contracting, and vendor management and insurance. FIs should utilize a multidisciplinary approach that takes advantage of security talent, legal talent and risk management professionals to craft a program addressing every aspect of security and privacy risk.

The time and investment for FIs to manage their risk and achieve compliance will not only put FIs in good standing with the law, such actions can enhance the "trust brand" of FIs. Comprehensive security/ privacy practices are needed not only to support new laws and regulations and mitigate legal liability, but can also be considered a source of competitive advantage. After all, customers who trust their FI and feel confident that their privacy is being respected and their personal information secured, will continue to be long-standing customers and be more inclined to buy services as their trust grows with a privacy-minded financial institution. If a FI's trust brand is marketed properly, it may also result in new customers who value protection of their personal information. These additional benefits can help make the costs of legal compliance more palatable to the organization on the whole.

***\*\*Disclaimer: Please note that this whitepaper is not intended to be a comprehensive summary of recent developments in the law, treat exhaustively the subjects covered, provide a complete listing of applicable laws, provide legal advice or render a legal opinion. Since the law is constantly changing and since the law will vary based on different facts and circumstances, statements in this whitepaper regarding the status of a given law or legal issue may not be current or applicable to your particular situation. You should not take any legal action based on the information in this whitepaper without first consulting an attorney.***