

## Address Telecommuting Risks

Many banks have not addressed the risks of telecommuting in their security and privacy plans.

If your bank allows telecommuting, even on an occasional basis, communicate to all employees the bank's policies and procedures for safeguarding information that leaves the office. A study by Ernst and Young found:

- › Technology-related policies and procedures are often overlooked when using home computers.
- › Sensitive information on home computers may be accessible to family members or others.
- › Most telecommuters connect to the Internet via consumer-class broadband or wireless, which may lack appropriate security protection.
- › Procedures for safeguarding and disposing of paper files may not be followed outside the office.
- › Even where security awareness training was provided to full-time telecommuters, occasional telecommuters were largely unaware of the need for addressing security issues at home.

### To address these risks:

- › Provide the necessary security mechanisms for home computers and peripherals before allowing employees to use them for work purposes; do not rely on employees to determine which security mechanisms to use.
- › Provide employees with locked cabinets and shredders, as well as guidance for handling paper records outside the office.
- › Provide awareness training to all employees, including those who occasionally work from home (currently and potentially in the future).
- › Monitor compliance with guidelines on at least an annual basis.

## NEW!! eRISK™ HUB HELPLINE/WEB SITE AVAILABLE TO INTERNET BANKING LIABILITY (IBL) CUSTOMERS

Progressive has contracted with **NetDiligence**, a cybersecurity and e-risk assessment company, to provide assistance to our customers who purchase IBL coverage.

The **eRisk Helpline** provides immediate triage assistance in case of a security breach. Initial calls are free of charge and include up to one hour of telephone support.

Any additional assistance will be billed directly to the bank.

The **eRisk Hub Web site** includes:

- › Directory of external resources with deep expertise in pre- and post-breach disciplines;
- › News Center for privacy and security news, blogs, risk management events, and helpful industry links; and
- › Learning Center for best-practice articles on compliance, network security, privacy and breach recovery.

If you are an IBL customer, visit [banks.progressive.com](http://banks.progressive.com) to access the eRisk Hub Web site. You should have recently received a reference card with your access code in the mail. If you do not have your access code, call Nicole at 800-274-5222, ext. 37580.

If your bank has not purchased IBL insurance, speak with your agent or underwriter about this important coverage.

### About NetDiligence

NetDiligence provides due diligence products to help clients determine how well their organization's network security and privacy practices measure up against known industry standards, as well as regulatory and insurance carrier requirements. Using proprietary methodologies and tools, NetDiligence provides a full range of enterprise-level information security, e-risk insurability, and regulatory compliance assessment and testing services.

## IN THIS ISSUE

- › Retaliation Claims on the Rise
- › Minimize Risk from Guaranteeing Customers' Signatures
- › Class Action Lawsuits Cite ATM Signage/Disclosure Issues
- › Six Steps to Better Privacy and Security Compliance



We know community banks.

For more loss control information or to view this SafeTalk® newsletter online, visit [banks.progressive.com](http://banks.progressive.com).

# Retaliation Claims on the Rise

**Progressive has seen a dramatic increase in retaliation claims over the past few years. The following situation that occurred at one of our community banks is an example of the types of retaliation claims that are being reported.**

Tina was hired as a teller and within a few years, promoted to assistant branch manager. Her performance reviews were very positive. She was then moved to fill a position at a different branch. Tina went willingly, but almost immediately had problems interacting with her new branch manager, Mark.

Tina alleges that Mark asked her on a date on several occasions during her first week at the branch. She alleges that after she refused, Mark began treating her unfairly; that she went to HR and complained about the situation; and that she told HR that she was the victim of sexual harassment. Six months later she was terminated. She claims that her termination was in retaliation for her complaints of sexual harassment.

The bank tells a different story.

Mark admits to asking Tina out on a date twice; but when she clearly was not interested, he never asked again, and denies treating her any differently as a result. He claims that after her mother was diagnosed with a serious illness, Tina's job performance began to suffer. He alleges that although the bank tried to make allowances knowing that she was going through a difficult time, Tina's performance eventually deteriorated to the point where he had no choice but to terminate her. Mark had no idea that Tina had complained to HR regarding his behavior.

The bank's HR representative, Hannah, stated that Tina had a discussion with her about her job situation. Hannah claims that Tina was aware that her performance was slipping due to her mother's illness and wanted the bank to know she was working on it. Hannah also claims that Tina was upset that Mark was not more understanding about her situation and was not allowing her more leeway to deal with her situation. Hannah alleges that she counseled Tina to find a

way to get her job done. She denies that Tina ever claimed that she was being sexually harassed.

After Tina was terminated, she filed a lawsuit against the bank, alleging sexual harassment and retaliation. The problematic allegation here is not the claim of sexual harassment since Mark's behavior is unlikely to rise to the level of sexual harassment. The potential exposure here arises from the retaliation claim. **Even if there were no sexual harassment, if Tina was retaliated against for making a complaint of behavior that she perceived as sexual harassment, she has a viable retaliation claim.**

The bank settled this case at mediation for \$50,000.

## Practice Tips:

### What Could the Bank Have Done Differently?

- › **Communication.** Improve communication between HR and managers. Here, Mark and Hannah each had parts of the story, but did not share information. They should have discussed the matter fully before any decision to terminate Tina was made.
- › **Accommodation.** Always explore what options may be available to deal with an employee situation. Could the bank have offered Tina part-time hours, flex time or a different position to help her through a difficult time? Some accommodation may have been enough to get Tina through a difficult time and back on track with her performance.
- › **Documentation.** Document performance issues honestly and completely. The bank's documentation here mentioned minor issues with Tina's performance, but did not accurately address how serious some of her lapses had been and the negative consequences that had occurred.



**Laura Simmons,**  
**EPLI Claims Manager**

Laura joined Progressive in 1992 after receiving her law degree cum laude from Case Western Reserve University School of Law. She received her bachelor's degree in English and political science from Wittenberg University. Laura deals primarily with employment-related claims and was involved in the development of Progressive's Employment Practices Liability Insurance Policy. She is a frequent speaker on employment-related topics.

The following article by **Barry M. Willoughby**, Partner and Chair of the Employment Law Section of Young Conaway Stargatt & Taylor, LLP., provides an update of recent court decisions that have expanded employees' rights.

## The Skunk at the Picnic

Human Resource professionals know how difficult it is to deal with a current employee who has filed a charge of discrimination against their employer. The situation is awkward at best. The employee is like "the skunk at the picnic." Management doesn't want to come near the employee for fear of being "sprayed" with the unpleasant aroma of a discrimination charge. This leaves the HR department in the unenviable position of dealing with the skunk and, of course, the inevitable "retaliation" claims.

The U. S. Supreme Court isn't making your life any easier. For several years, the Court's decisions have broadened the rights and remedies of employees who file charges of discrimination against their employer. The decisions from the Court this term continue that trend.

Most federal and state anti-discrimination statutes contain provisions prohibiting retaliation. According to statistics compiled by the Equal Employment Opportunity Commission (EEOC), retaliation claims are proliferating across the country. The number of retaliation claims filed with the EEOC has more than doubled over the past 10 years. Retaliation claims now constitute a startling 30% of all charges filed.

Starting in 2006, the United States Supreme Court expanded the rights of employees in several decisions dealing with statutory anti-retaliation provisions. In *Burlington Northern & Santa Fee Railway Co. v. White*, 126 S. Ct. 2405 (June 22, 2006), the Supreme Court held that an employee bringing a retaliation claim need not show that the adverse action taken by his or her employer impacted "compensation, terms, conditions, or privileges of employment." Instead, the Court established a much lower burden of proof. The employee need only demonstrate that a "reasonable person" in the same position would have been dissuaded from exercising his or her statutory rights as a result of the employer's actions, even if the actions were unrelated to the workplace.

The trend toward expansion of employee rights has continued this year. First, in *CBOCS West, Inc. v. Humphries* ("Cracker Barrel"), the Supreme Court determined that employees can state a claim for retaliation under a reconstruction era law called "§1981." The Court concluded that an anti-retaliation provision was implicit in the law even though it contains no explicit provision. The decision is significant because Section 1981 differs significantly from Title VII in that it has a longer statute of limitations, no limitations, or caps, on recovery of damages, and applies to employers of all sizes. Second, the Supreme Court, in *Gomez-Perez v. Potter*, held that section 633a (a) of the Age Discrimination in Employment Act (ADEA) prohibits retaliation against a federal employee who complains of age discrimination.

The most significant case had not been decided as of the date this article went to press. *Crawford v. Metropolitan Government of Nashville and Davidson County, Tenn.*, will address the scope of protection for employees who are interviewed in connection with an internal investigation. Most Court observers, including the authors, believe that the Court will conclude that broad protection of employees is required in such circumstances.

Given the recent judicial expansion of employee rights discussed above, and the proliferation of retaliation charges being filed, what can a prudent employer do to deal with "the skunk at the picnic"?

Our suggestions are: (1) audit your employment policies; (2) train your managers and supervisors in how to conduct performance reviews and discipline employees; (3) consistently apply your policies; (4) exercise caution when investigating complaints of retaliation and document the basis for disciplinary action; and (5) provide for objective internal review before dismissal.

The expansion of employee rights and the proliferation of retaliation charges looks set to continue, leaving you to deal with the inevitable "skunk at the picnic." However, by taking the steps outlined above, you can make dealing with the "skunk" a less unpleasant experience, and reduce your company's potential liability in the process.



# Six Steps to Better Privacy and Security Compliance

By **Mark Greisiger** and **David Navetta**, NetDiligence

**Mark Greisiger** is the president of NetDiligence, a leading cybersecurity assessment services firm and a PCI Approved Scanning Vendor (ASV). Mark is an authority on cybersecurity and network risk for computer-dependent businesses, government agencies and financial institutions.

**David J. Navetta, Esq.**, CIPP is an attorney with over a decade of legal experience, including in the areas of contract drafting, litigation, insurance law, and information security and privacy compliance. Founder and Managing Member, InfoSecCompliance, LLC, Mr. Navetta is a Certified Information Privacy Professional (CIPP) through the International Association of Privacy Professionals.

Over the past several years, there seems to have been a dramatic increase in the incidence of security breaches, and the loss and misuse of private customer information, credit card numbers and other sensitive data. Are there really more security breaches today than a decade ago or are data breaches simply being reported today whereas a decade ago they were not disclosed?

It's both. Indeed, there are more security breaches today than a decade ago. Businesses, schools, financial institutions, organizations and the government all capture and use more personal (sensitive) information than before. As a result, personal data about customers, members and citizens is growing in value, and as this data grows in value, the risks increase as well. This has caused elected officials to pass more laws to address consumer privacy risks.

Some of the more recent legal and compliance risks arising for the banking industry include compliance with breach notice laws, merchant bank liability for payment card security breaches and failure to comply with the Payment Card Industry Data Security Standard (PCI DSS) and the FACTA Identity Theft Red Flag Rules.

So, what can you do to ensure that your daily business operations comply with your privacy and security policies as well as applicable laws and regulations? Here are six things you can do immediately to improve your security and privacy posture and reduce your overall risk.

## 1. Know your data.

The first step in protecting personal data is to determine what data exists and whether or not the information is necessary to accomplish the business purposes for which it is being collected. Too often businesses collect and retain personal information – Social Security numbers, birth dates, credit card numbers – even though they are not necessary to accomplish a business purpose. Your first step should be to ask if particular information is necessary. If it isn't, don't collect the data. If the data is necessary, you should document why it is necessary and how long it is needed. Once the information is no longer required for the identified business purpose, it should be destroyed.

## 2. Know your institution.

Obtain an independent, enterprise-wide e-risk assessment that

evaluates the people, processes and technology underlying your security and privacy posture. An objective, third-party assessment allows you to identify specific vulnerabilities and legal liabilities, so you can focus on hardening security precisely where it's needed. In other words, it ensures that you spend your security budget on necessities, not luxuries. The assessment should include a third-party penetration test to evaluate whether Internet-facing systems are capable of deflecting the known hacker exploits that threaten financial institutions.

## 3. Know your people.

Personal information is collected, processed and used throughout every aspect of banking operations. As such, many people are involved with how customer information is collected and processed. The same holds true for compliance. There is no one person or position that can achieve full compliance with information security and privacy requirements. Security professionals, IT staff, lawyers, risk managers, CFOs, CEOs, and public relations personnel all have roles and must provide input. Financial institutions should establish cross-disciplinary working groups to address these issues. The members of the group should "translate" their issues and concerns so that others in the group gain an understanding of what needs to be done. Coming at this solely from an IT or legal perspective will not work.

## 4. Know your providers.

You have an obligation to use suppliers and processors that are competent to adequately protect your institution's sensitive information. This requires that you have a basic knowledge of the capabilities of your providers, how their personnel are trained, and what processes and procedures they have in place to protect your data. Verify that the data is either returned or destroyed when it is no longer needed.

Make sure you have attorneys working with security professionals to interpret privacy and security laws and put policies and procedures in place that comply with those laws. Attorneys should also be engaged to address external contractual relationships with service providers, including drafting privacy and security contract terms to establish security controls, incident response, enforcement and monitoring, and transferring risk of loss.

continued on page 6 >>

## Class Actions Against Community Banks Cite ATM Signage and Disclosure Issues

Class actions are being brought against community banks by The Consumer Advocacy Center (CAC), a private Chicago law firm that claims on its Web site to help clients “vindicate their rights against banks who charge deceptive late fees... and other businesses that attempt to take advantage of the ordinary consumer.”

**In a recent case, an Illinois bank settled an ATM disclosure action for \$113,750, plus payment of \$86,250 in attorneys’ fees to the CAC. Similar cases are being filed around the country.** The suits allege violations of the EFT Act, Reg E, the Expedited Funds Availability Act and Reg CC.<sup>1</sup>

They allege that the banks failed in their statutory duty to post fee notices externally next to each machine, as well as fee and withdrawal restriction notices on the ATM screens themselves. The statutes require notice of the fee amounts and notice that any funds deposited may not immediately be available for withdrawal. In some cases, notice was posted on the screens, but not on the physical ATM. In one case,

signage on the ATM had been vandalized; the bank now has to prove it had no opportunity to replace the stolen fee notice signs in order to defeat the monetary consequences which the statutes impose.

To avoid compliance issues and potential class action exposure, schedule a physical inspection of all ATMs to ensure that they contain appropriate disclosures on all ATM screens and external surroundings. Additionally, if the bank has raised any of these fees, all screen signage must provide notice of the current and actual fees charged.

<sup>1</sup> Settlement agreement available on the CAC Web site. Specific statutory references for your legal or compliance departments to review are:

- › 15 USC § 1693b(d)(3) and 12 CFR § 205.15(c);
- › 15 USC § 1693b(d)(3)(C), and Reg. E, 12 CFR §205.16(e); and
- › 12 USC § 4004(d)(2) and 12 CFR §229.18(c)(1)

## Minimize Risk from Guaranteeing Customers’ Signatures

**Bank employees guaranteeing signatures on stock transfers should be reminded that every decision to guarantee a signature in the bank’s name exposes the bank to potential liability, which extends beyond simple confirmation that the signature is genuine.**

The Uniform Commercial Code provides that a person guaranteeing a signature warrants that at the time of signing:

1. the signature was genuine;
2. the signer had legal capacity to sign; and
3. the signer was an appropriate person to endorse the security.

If a security is wrongfully transferred in reliance on the bank’s guarantee, the issuer and its transfer agent can sue the bank for loss resulting from a breach of any of these warranties.

Guaranteeing signatures should be restricted to bank officers, and the following guidelines should be reinforced to all guarantors periodically to minimize the bank’s exposure.

### Signature Guarantee Guidelines\*

#### A. Warranty that the Signature Is Genuine

1. **Only guarantee signatures of customers.** Ideally, direct the customer to an officer who is personally familiar with the customer.
2. **Always compare the signature on the endorsement** with the signature card or brokerage account application on file for the customer. Signatures where no signature card is on file should be guaranteed only at the direction of an officer who knows the customer.

3. **Require proper identification with picture ID.**
4. **Insist on the appearance in person of every person** whose signature you are guaranteeing. Never guarantee a signature at the request of a person other than the actual signer.

#### B. Warranty that the Signer Has Legal Capacity to Sign

Make sure there is no question that the person whose signature you are guaranteeing is of **legal age** (18 in most states) **and competent**. Refuse to guarantee if you know that there has been a legal adjudication of incompetence or if you have serious doubts about the person’s ability to understand.

#### C. Warranty that the Signer Is an Appropriate Person to Endorse the Security

1. **Ask to see the certificate** to determine how it is registered. In the case of mutual funds or other book entry securities, ask to see a copy of the most recent statement reflecting the registration of the security.
2. **Do not guarantee a signature on a blank stock or bond power.** The name of the issuer and the number of shares should be filled in on the power.
3. Where more than one name appears, **refuse to guarantee unless all owners are physically present and sign in your presence.** If an owner is out of town, use a “Securities Specific Power of Attorney for Multiple Security Owners.” ([Download at www.kemark.com/downloads.html](http://www.kemark.com/downloads.html).)

continued on page 6 >>

## Minimize Risk from Guaranteeing Customers' Signatures , continued

4. There are more complicated legal issues and requirements where **one of the owners has died** or the requestor is a **Joint Tenant, Life Tenant or individual signing as a Fiduciary or Attorney-in-Fact**. Similarly, signatures on **securities registered in the name of a corporation, partnership or limited liability company** and signatures by **individuals purporting to act on behalf of unincorporated associations** raise specific issues to be addressed. To ensure compliance in these situations, consult Legal Counsel.

### D. Additional Legal Guidelines

1. **A signature guarantee may not be qualified in any way.** Never append a date or any other terms of limitation or explanation next to the Medallion Stamp.
2. **Never affix the Medallion Stamp on a Power of Attorney, Trust Agreement or any document other than a security.** Refer all such requests to Legal Counsel.
3. If you are asked to guarantee a stock power by a **customer who is unable to write his or her name**, the customer should endorse by means of a mark ("X"), accompanied by the signatures and addresses of two witnesses (neither of whom is the transferee of the security), and a written statement by the witnesses that "the transfer instrument was read to the transferor in our presence, that he or she made his or her mark in our presence and that he or she signified an intention thereby to transfer the security." All such requests should be referred to Legal Counsel.
4. **"Endorsement Guaranteed," "Signature(s) Specially Guaranteed" and "Instruction Guaranteed"** extend warranties far beyond the usual

signature warranties and should never be executed. (The UCC forbids an issuer from requiring these.)

5. **SEC Regulations** impose special requirements whenever securities worth more than \$10,000 come into the possession of a broker-dealer or bank **from someone other than the registered owner**.
6. It is imperative that you **make and retain copies of all signature guarantees and supporting documentation** (such as Powers of Attorney, board resolutions, Letters Testamentary, drivers' licenses, etc.).
7. **Only authorized officers, branch managers, assistant branch managers and customer service managers should have access to Medallion Stamps.** The importance of proper safeguards and security procedures for the bank's Medallion Stamps cannot be overemphasized to avoid potential fraud.
8. **The Medallion Signature Guarantee Imprint was created for use exclusively within the context of specific transactions** involving the sale, transfer, liquidation, or change in ownership of securities. Guarantors may be placing themselves at risk when using Medallion Signature Guarantees for purposes outside the scope of the Medallion Program documents, and guarantors are urged not to do so.

For more information about the bank's responsibilities with regard to signature guarantees, consult Legal Counsel or your institution's Medallion coordinator.

For information about Progressive's STAMP Surety Bond program, call or have your agent call Progressive at 800-274-5222.

\* This article provides a summary of guidelines published by the American Bankers Association. The full text is available at [http://www.aba.com/aba/documents/securities/Medallion\\_procedures.pdf](http://www.aba.com/aba/documents/securities/Medallion_procedures.pdf).

## Six Steps to Better Privacy and Security Compliance, continued

### 5. Know the law.

With the complex patchwork of privacy and security laws that exist in the U.S. (local, state, federal and international law are often at issue), even identifying which laws apply can be difficult. Once applicable laws are identified, they need to be analyzed to see how and where they may impact your institution. In some cases, it may be possible to find commonalities between privacy and security laws and streamline compliance. Other times, costly remediation may be required to address multiple compliance regimes. While this process can be daunting, it is a prerequisite to achieving a legally compliant organization.

### 6. Know your risks.

No matter what measures you take or how much you spend on training, network security or physical safeguards, residual risk will always exist. Consider transferring the remaining risk through network and privacy liability coverage. With this approach, you reduce your overall expense for network security and privacy protection. Remember, however, while you may be able to transfer financial risks, you can't transfer the duty to implement and maintain appropriate safeguards and your insurance company will require a baseline of reasonable security.

Unfortunately, it is likely that most of us will experience a breach incident despite our best efforts. Financial institutions that have taken the appropriate measures beforehand will be able to minimize the damage. Only when you implement an ongoing program for data protection can your institution effectively walk the tightrope between privacy, security, and legal risk.