For Release Upon Delivery
2:30 p.m., March 10, 2005

TESTIMONY OF

AMY S. FRIEND

ASSISTANT CHIEF COUNSEL

OFFICE OF THE COMPTROLLER OF THE CURRENCY

Before the

COMMITTEE ON BANKING, HOUSING AND URBAN AFFAIRS

UNITED STATES SENATE

MARCH 10, 2005

Statement Required by 12 U.S.C. § 250:

The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

Mr. Chairman, Ranking Member Sarbanes, and members of the Committee, the OCC appreciates the opportunity to testify today about a subject that is critically important to the integrity of the relationship between a bank and its customers – a bank's ability and legal obligation to safeguard customer information. We commend the Senate Banking Committee's leadership in addressing this important subject.

It is a matter of primary importance to the OCC, as it is to the Committee, that national banks have adequate procedures in place to safeguard customer information. My testimony will describe the legal requirements on banks to safeguard customer information, the examination process for assessing the adequacy of a bank's security program, OCC enforcement actions against banks and individuals for breaches of information security, and upcoming interagency guidance that will detail the circumstances under which the federal banking agencies expect institutions to notify their customers of security breaches.

Background

The OCC routinely examines national banks for the safe handling of customer information. We consider safeguarding customer information to be essential to maintaining the safe and sound operations of a bank. As a result, information security has been a part of our overall supervisory process for many years. The level and extent of our supervisory review has evolved as bank operations and the technology banks employ have become increasingly complex and sophisticated. The OCC has a number of examiners dedicated full-time to conducting information technology and information security examinations, as well as many additional examiners performing these functions for a portion of their time.

Over the years, the OCC, on its own and in conjunction with the other bank regulators, has published guidance and handbooks in this area advising banks of our expectations about acceptable risk management processes and procedures for safeguarding information, including in the areas of maintaining, transporting, and disposing of information. Further, OCC examination staff and attorneys participate in interagency coordination meetings concerning information security, such as regularly attending and participating in the Attorney General's Council on White Collar Crime, Subcommittee on Identity Theft.

Information Security Guidelines

Section 501(a) of the Gramm-Leach-Bliley Act states that each financial institution has an affirmative and continuing obligation to protect the security and confidentiality of customer information. Under section 501(b), the federal financial institutions regulators are directed to establish standards for financial institutions relating to the administrative, technical, and physical safeguards of that information in order to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

To carry out this broad mandate, in February 2001, the OCC and the other federal banking agencies issued standards in the form of guidelines, requiring each bank to have a written information security program designed to meet these statutory objectives.

Under these security guidelines, the board of directors must approve a bank's written information security program and oversee its development, implementation, and maintenance. The Board must review annual reports on the status of the program and the bank's compliance with the guidelines.

In developing its information security program, a bank must assess the risks to its customer information and any methods the bank uses to access, collect, store, use, transmit, protect, or dispose of customer information. A bank must identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure or misuse of its customer information, assess the likelihood and potential damage of these threats taking into account the sensitivity of customer information, and assess the sufficiency of policies, procedures, and systems the bank maintains to control the risks.

The bank must then design its information security program to control the identified risks. Each bank must consider at least the eight specific security measures set forth in the guidelines and adopt those that are appropriate for the institution. These measures include access controls on customer information, encryption of electronic information, monitoring systems to detect actual and attempted attacks on customer information, and response programs that specify actions to be taken when a bank suspects or detects unauthorized access to customer information.

Each bank must train staff to implement the program and oversee its arrangements with service providers that have access to bank customer information. This includes using due diligence in selecting service providers, requiring by contract that service providers implement appropriate safeguard measures, and monitoring the activities of service providers where necessary to control the risks the bank has identified that may be posed by the service provider's access to the bank's customer information.

A bank's information security program must not be static. Banks must routinely test their systems and address any weaknesses they discover. Banks must adjust their programs to address new threats to customer information, changes in technology, and new business arrangements.

Examinations for Information Security Programs

The OCC examines national banks for compliance with the security guidelines. In conducting an examination, an examiner will review the bank's written information security program and its implementation in accordance with interagency examination procedures. These procedures include the following determinations:

- whether the program is appropriate for the size and complexity of the bank and the nature and scope of its activities;
- the degree of the board's involvement in overseeing the program;
- the adequacy and effectiveness of the bank's risk assessment, including whether the bank has considered risks to all methods to access, collect, use, transmit, protect, and dispose of information;

- the adequacy of the program to manage and control the identified risks, including technical and procedural controls to guard against attacks, encryption standards used, and monitoring systems;
- whether staff are adequately trained to implement the security program;
- the nature and frequency of tests of the bank's key security controls, the results of these tests, and whether they are conducted or reviewed by independent sources;
- the adequacy of measures to oversee service providers; and
- whether the bank has an effective process to adjust its information security program as needed to address such matters as new threats, the sensitivity of customer information, technology changes, a bank's changing business arrangements, and outsourcing arrangements.

OCC Enforcement Actions and Investigative Activities

From time to time, things can go wrong and customer information may be compromised despite a bank's information security program. The program itself may be inadequate, the systems to protect customer information may be breached, bank employees may not follow the program requirements, or unanticipated risks may arise. An outside service provider that maintains bank customer information on the bank's behalf may face the same issues. Where the OCC finds the bank, the bank's employees, or the bank's service provider to be at fault, the OCC can bring an enforcement action.

Supervisory and Enforcement Actions Against Banks

The OCC has taken various actions to enforce compliance with the security guidelines against banks. In some cases, where the bank had not already done so, the OCC required national banks to notify their customers of security breaches involving their personal information. In another circumstance, the OCC directed a national bank to revamp its employee screening processes.

For example, the OCC issued a Cease and Desist Order against a California-based national bank, requiring, among other things, that the bank notify customers of security breaches, after the OCC's investigation revealed that the bank's service provider improperly disposed of hundreds of customer loan files. The OCC also issued a Cease and Desist Order against the bank's service provider, and assessed hundreds of thousands of dollars in civil money penalties against the bank and its service provider.

In another case, the OCC, after investigating allegations of a data compromise by a bank employee, directed a retail credit card bank to notify customers whose accounts or information may have been compromised. The OCC was able to determine that the information was used for nefarious purposes, after working collaboratively with the Federal Trade Commission to review complaints of identity theft made to the Commission through its Consumer Sentinel Program, of which the OCC is an information-sharing member.

The OCC also directed a large bank to improve its employee screening policies, procedures, systems and controls after the OCC determined that the bank's employee screening practices had

inadvertently permitted a convicted felon, who engaged in identity theft related crimes, to become employed at the bank. Deficiencies in the bank's screening practices came to light through the OCC's review of the former employee's activities. OCC examination staff and attorneys regularly discuss appropriate employee screening practices and processes with national banks.

Investigations and Enforcement Actions against Bank Insiders

In more than fifteen other cases, the OCC has taken enforcement actions against bank insiders who have breached their duty of trust to customers, were engaged in identity theft-related activities, or were otherwise involved in serious breaches or compromises of customer information. These enforcement actions have included, for example, prohibiting individuals from working in the banking industry, personal cease and desist orders restricting the use of customer information, the assessment of significant civil money penalties, and orders requiring restitution.

For example, after the OCC investigated and determined that a Colorado-based bank loan officer and loan processing assistant misappropriated customer information and emailed the information to a third party, the OCC prohibited the two individuals from the banking industry, assessed civil money penalties against each, and issued cease and desist orders against each that placed restrictions on their future use of customer information.

In another matter involving a collections supervisor of a bank, the OCC's investigation revealed that the former bank employee misappropriated customer information, created fictitious Paypal

payment accounts, and then embezzled money from the customers' bank accounts, thereafter depositing the money into the fictitious Paypal accounts. The OCC prohibited the employee from the banking industry, the employee paid tens of thousands in restitution, and the OCC assessed a civil money penalty against the employee.

Many of these data compromise or identity theft cases were initially processed as part of the OCC's Fast Track Enforcement Program, whereby the OCC specifically targets current or former bank insiders for enforcement action based upon criminal authorities' declining to prosecute. Typically, law enforcement relies upon loss amounts in deciding whether to prosecute. However, loss amount from theft of customer information is both difficult to quantify and may not be present for the institution from which the information has been misappropriated. In such cases, the OCC has acted to remove wrongdoers from the industry, and, in appropriate circumstances, ordered restitution and civil money penalties as well. The OCC was also involved with the recent amendment of the Suspicious Activity Report ("SAR") form to include a specific check box for identity theft, thereby making it easier for criminal law enforcement and the federal banking agencies to identify referrals concerning identity theft and data compromise.

Upcoming Guidance on Response Programs and Customer Notice

The OCC believes that notifying customers of a security breach involving their personal information is a key part of a bank's affirmative duty under the security guidelines to protect customer information against unauthorized access or use. While a bank may monitor a customer's account for suspicious activity following an incident of unauthorized access to that

customer's information, monitoring will not prevent an identity thief from misusing that customer's personal information at another institution, such as to open a new account at a different bank. Armed with notice, however, bank customers may take steps to protect their information from further misuse, such as by placing fraud alerts on their credit reports that will alert other creditors that these individual may be victims of fraud.

The information security guidelines, however, do not specifically require banks to notify their customers in the event of security breaches involving their personal information; therefore, the OCC is working with the other federal bank regulators to finalize interpretative guidance stating the agencies' expectation that banks notify their customers of security breaches in appropriate circumstances. I am pleased to inform the Committee that, after considering public comments, the agencies reached an agreement on this guidance last week. The Acting Comptroller of the Currency approved the guidance on behalf of the OCC earlier this week, and the other agencies are now working through their approval processes.

The OCC, along with the other banking regulators took the initiative to propose the guidance in 2003 as an interpretation of the security guidelines. Noting that internal and external threats to a bank's customer information are reasonably foreseeable, the guidance stated that the agencies expect each bank to implement a response program with specific policies and procedures for addressing incidents of unauthorized access to customer information. Specifically, the guidance described the components of a bank's response program. It stated that a bank should assess the nature and scope of the security breach, take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of the customer information, notify law

enforcement and the bank's primary regulator of the incident, and notify customers of the incident when warranted, as well as provide customers with helpful information about how to contact the bank with questions and how to place a fraud alert on consumer reports.

The guidance provided that customer notice is warranted when the security breach involves access to information of the type that could easily be misused, such as a customer's social security number and account number, which could be used by an identity thief to impersonate an individual and take over the customer's account. The guidance stated that banks are expected to notify their customers of the security breach unless they determine that the breach is unlikely to result in misuse of the customer information.

In crafting the standard for customer notice the agencies have sought to establish the appropriate threshold for when customers may actually benefit from receiving notice. For instance, under the proposed guidance, notice would not be warranted where a bank can immediately contain a security breach and establish that the information has not been and is unlikely to be misused. An example of this would be where a bank determines that customer information was destroyed before it could be retrieved or used.

The agencies received a number of comments on the proposed guidance emphasizing that not every breach of information security will result in harm to customers. Commenters stated that providing an overabundance of notices to consumers may have unintended consequences – mainly that consumers may initially be alarmed and perhaps monitor or close their accounts, or place a fraud alert on their credit reports, but eventually may be lulled into complacency by a

proliferation of notices. Moreover, commenters maintained that notifying customers of security breaches in every instance could result in the unnecessary placement of fraud alerts on consumer reports and, over time, erode the usefulness of fraud alerts. The agencies agree that some potential for misuse of a customer's information should be present to trigger notice to that customer.

A number of commenters recommended permitting a delay of notice to customers while a law enforcement investigation is pending to avoid compromising the investigation. California law provides for a delay of customer notice if the notice would impede a criminal investigation. The agencies have taken into consideration these and other comments in finalizing the guidance.

Enforcement of Noncompliance with the Guidance

The OCC will consider a bank's failure to follow the final guidance as noncompliance with the underlying security guidelines. The OCC has several enforcement options available to address noncompliance. One option is to use the safety and soundness enforcement process provided by federal law and OCC regulations. Under this process, the OCC would issue a notice to the bank detailing deficiencies and requiring the bank to submit a corrective action compliance plan within 30 days. An acceptable plan could provide that the bank will adopt measures to correct deficiencies, including notification to customers and restitution for any loss caused by the bank's conduct. If the bank failed to submit an acceptable compliance plan, or failed to materially comply with its compliance plan, the OCC could then issue a Safety and Soundness Order. A Safety and Soundness Order is a formal, public document that is the legal equivalent of a Cease and Desist Order. If a bank fails to comply with such an order, the order may be enforced in

federal District Court and the bank could be assessed civil money penalties. The OCC could also choose other enforcement options to address a bank's failure to comply with the guidelines, such as issuing a Cease and Desist Order, or assessing civil money penalties.

Conclusion

Mr. Chairman, through the Gramm-Leach-Bliley Act, particularly section 501(b), Congress gave the regulators the direction and important authority to establish information security standards for use by the financial institutions we regulate. The OCC has found this authority to be well suited to address the evolving information security challenges we face. We are committed to using this authority to assure that national banks have adequate procedures in place to safeguard their customers' information. Thank you.