Statement of David B. Watson

Chairman, Merrick Bank

before the House Committee on Financial Services

Subcommittee on Oversight and Investigations

regarding Security of Credit Card Data Processing

July 21, 2005

Madam Chair, Mr. Gutierrez and Members of the Subcommittee:

On behalf of Merrick Bank, thank you for the opportunity to testify before the Subcommittee on the issue of credit card security. As a cardholder and as Chairman of a card-issuing bank, I commend this Committee for its diligence and interest in formulating good public policy on a topic of intimate importance to virtually every American. Merrick Bank is a Utah financial institution, subject to regulation and annual examination by the FDIC and the Utah Department of Financial Institutions. We issue credit cards to account holders, and we make payments of processed credit card transactions to merchants. Both services are important to our customers and to the merchants, and we apply stringent privacy and data integrity standards to both. Credit card and account holder security is a fundamental principle of our business. It has to be.

The specific subject of this hearing is data security. There have been several well-publicized financial data security breaches over the past few months, the most recent involving the credit card transactions processor CardSystems Solutions. Merrick is one of at least seven banks which make payments to merchants who use CardSystems for processing. Although any potential breach of private data raises serious issues, the nature of merchant card processing does limit the

amount of data, which might be exposed by the processor. The merchant processor does not typically have the kind of personal identifying information of the cardholder which would precipitate identity theft; rather it has transaction data, which could be used to perpetrate fraudulent transactions. It is unknown at this point the extent to which the CardSystems breach has resulted in any attempted fraudulent transactions and, like other card issuing banks, we are aggressively monitoring accounts to detect any potential fraudulent transactions.

Today we will describe the card payment process, the specifics of the background and breach by CardSystems, and detail our actions, both regarding CardSystems and with any card processor we use.

Any bank's involvement with credit cards is as a partner with other key players in the transaction chain. Each entity involved in credit cards, including card issuing banks, merchants, card processors, transaction payment banks, and Visa and MasterCard must properly and accurately fulfill its role to assure the protection of the consumer. The integrity and security of the process is strong when the performance by each party is strong.

To most consumers, the credit card system is simple and dependable. But behind the consumer's view of that simple process of charging a purchase, there is a sophisticated series of steps involving several players for each transaction, a series of steps that is repeated millions of times daily.

Most consumers are generally aware of how a credit card is issued. Consumers apply and, after approval, are issued credit cards by financial institutions. This process is reasonably straightforward in terms of data security. In most cases the consumer's billing information is maintained by the issuing institution and used to generate monthly statements and to record payments. The issuing bank must ensure the security of its own credit card program. Merrick Bank is a significant issuer of credit cards. This security issue, however, arose not with the issuing part of the credit card system, but with the merchant transaction processing part. We and other banks make payments to merchants who use CardSystems for processing.

Maintaining and upgrading our card data security systems is a major priority, and must be for any financial institution. Our commitment to the industry standards of security in this field is reflected by our insistence that CardSystems meet the formal Visa accreditation standards before we began our business relationship with them, and our aggressive steps to investigate the problem and assure immediate remediation after we were informed of the data breach by CardSystems on May 25, 2005. We are committed to ensuring that any processors with whom we work are compliant with the industry standards of data security. We want to work with the Committee and other participants in this process toward improvements that would help ensure that systems we work with will protect consumer data. As technology advances, so inevitably does the sophistication of hackers and others who attempt to misuse or breach the technology.

It is useful to describe the broad picture as to how card processing works in general and in our experience. Credit card transaction processing is a multi-party transaction, involving not only card holders, merchants and their processors, but also the card issuing bank, the merchant

payment bank, and the card associations. The merchant either does business directly with the processor or, particularly for smaller merchants, through an independent sales organization (ISO) which aggregates many small merchants and arranges for their processing. The cardholder initiates the transaction with the merchant. The processor performs the "back office" operation of seeing that the transaction is authorized, sending notice for payment to the cardholder's bank, and ensuring that the merchant is paid for the transaction. In some cases processing agents are themselves banks and can make the payments. In many cases the processor or the ISOs have agreements with banks to make the payments of approved charges to merchants. The paying bank is reimbursed by the card issuing bank through the Visa or MasterCard settlement network.

All of these operations are conducted according to rules imposed by the Visa and MasterCard Associations and other card systems. In the case of CardSystems, its transactions predominantly involve Visa and MasterCard acardholders. The Associations reserve the right to approve the issuers of cards and the processors of card transactions. The Association rules dictate standards for card processing. They set forth the procedures which merchants and processors must use for processing various types of transactions, including handling fraudulent transactions.

Aside from this regulation of typical day-to-day transaction activities, Visa and MasterCard have developed, over the past five years, a specific accreditation program for card processors. As of January 1, 2005, Visa, MasterCard, American Express, and Discover have agreed on one set of criteria, Payment Card Industry (PCI) Data Security Standards, to unify the standards and certification processes, which had developed separately over the past few years. PCI approval must be certified by an outside auditor, which itself is certified by Visa, MasterCard and the

other card companies as eligible to make a PCI assessment. After the initial PCI approval, card processors are required to undertake an annual audit, again to be performed by an Association-approved reviewing firm. Should there be disputes about activities of any participants in the card processing system, which include merchants, processors, and paying banks, the Associations reserve the right to determine remedies against various parties.

With that background, I will describe Merrick's perspective on the CardSystems Solutions events.

Merrick has been working with merchants and card processors for more than five years. In September 2003, we were approached by representatives of CardSystems regarding the development of potential business with CardSystems and regarding the transfer of certain ISO contracts to Merrick from Provident Bank. CardSystems was a known entity in the card processing field, having been engaged in card processing with a number of banks for several years. CardSystems was doing business with at least five other banks in addition to Provident Bank. We did not have any significant business contacts with CardSystems before 2003. During a preliminary due diligence review following those 2003 discussions, we determined that CardSystems was not CISP certified by Visa. CISP, the Cardholder Information Security Program, was VISA's data security standard and accreditation process prior to the adoption of today's PCI data security standards. Visa had implemented the CISP standards in 2001, and was allowing processors like CardSystems until September 30, 2004 to secure this CISP certification. We advised CardSystems that we would not consider participating in any processing transactions with CardSystems until and unless CardSystems became CISP certified.

CardSystems engaged an auditor, Cable & Wireless Security, from the Visa-approved auditor list to conduct the CISP assessment. That assessment appears to have begun in 2003, while our predecessor Provident Bank was acting as a merchant payment bank for CardSystems. Cable & Wireless was selected by CardSystems and paid by CardSystems. The audit report was sent by Cable & Wireless to Visa. Cable & Wireless reported to CardSystems and to Visa that CardSystems had taken the necessary steps to be compliant with Visa's CISP standards. In June 2004 Visa informed CardSystems that it deemed CardSystems an approved Association processor, CardSystems so advised Merrick, and we then confirmed with Visa.

The Cable & Wireless "Visa U.S.A. Cardholder Information Security Program (CISP) Service Provider Report on Compliance" (the Report) stated that CardSystems

> has implemented sufficient security solutions and operates in a manner that is consistent with industry best practices and the intent of Visa's CISP program. CardSystems is dedicated to protecting the security of their customer' [sic] information and approaches the process of security with determination.

Further, the Report concluded that

> [t]he results of this assessment will provide CardSystems and VISA U.S.A. with valuable assurance that appropriate precautions have been taken to secure sensitive cardholder data, and will assist in upcoming annual compliance audits.

The Report asserted that the audit included a thorough evaluation of CardSystems' operating environment, including "all systems and network components that retain, store or transmit cardholder data". The Report stated that the Security Engineers completed their review by complying with Visa's standards, performing assessments on the selected systems outlined in the Visa U.S.A. CISP Security Audit Procedures and Reporting and utilizing Visa's *Testing Procedures* as the primary guide to evaluate CardSystems for compliance with the CISP.

With CardSystems having met our requirement to become CISP certified, as determined by the auditor and Visa, we negotiated with Provident Bank and other parties over the assignment of their merchant payment contracts and ISO agreements. These negotiations were successful, and the assignment of payment responsibilities from Provident Bank to Merrick was effective September 30, 2004.

From that point to May 2005, Merrick's payments for the transactions presented by CardSystems proceeded routinely. On May 22, 2005, CardSystems identified a security breach in its operation, and on May 23 contacted the FBI. On May 25, CardSystems contacted Merrick and advised us of a possible intrusion and export of cardholder data at CardSystems. Merrick reviewed this information and notified VISA and MasterCard of the potential security breach. On May 27, 2005, with the approval of VISA and MasterCard, Merrick engaged Ubizen (a well known forensic IT audit firm) to thoroughly investigate the security breach at CardSystems, and Ubizen began an onsite examination of CardSystems at its Tucson facility on May 31, 2005. We also sent our Chief Security Officer and Senior Network Engineer to the CardSystems site to investigate the issue and see that immediate action was taken to prevent any further data breach.

The forensic audit has identified two issues at CardSystems which, in combination, made this breach possible. First, CardSystems retained certain transaction data on their system in clear violation of Association rules. These data retention practices were inconsistent with CISP standards, and it is unclear to us why the Cable and Wireless Report did not note any objection to

the practice, which was ongoing when the CISP certification was approved by Visa in 2004. Ubizen reports this data retention practice had been followed by CardSystems since 1998.

Second, Ubizen identified certain issues with CardSystems servers and software, which were compromised by the intruder. The Cable & Wireless Report did not make any mention of these system vulnerabilities. Ubizen reports that CardSystems servers showed evidence of unauthorized activity as early as April 2004. The Ubizen report does not confirm, however, any actual data export until May 2005. It has been reported that as many as 40 million accounts may have been exposed. That estimate is based on the number of unique accounts authorized by CardSystems from August 2004 to May 2005. The investigation of exactly how much data was actually exported confirms only one export of information on about 263,000 cards. This is a serious and troublesome breach to be sure, and we are committed to dealing aggressively with any breach regardless of the number of cardholders involved.

Merrick, Ubizen, CardSystems, Visa and MasterCard have been aggressively working together to see that the IT issues permitting the breach are corrected and that the CardSystems data environment is firmly secured. Visa and MasterCard have identified the cardholders whose accounts they believe may have been compromised and have sent notice to the issuing banks of the potentially affected cardholders. This was accomplished by June 17, 2005.

Merrick is taking three further steps. First, in consultation with the Associations we have carefully evaluated the findings of the forensic auditor and required CardSystems to immediately address the issues the assessment has raised. Second, Merrick, immediately upon being notified

of the breach, initiated a search for alternate processors to serve our client merchants. Finally, in consultation with security and data experts, Merrick is developing its own set of requirements for card processors for whom we make payments to assure their compliance with all applicable card association standards. For example, not only will processors have to be current with the PCI certification and annual audit requirements, but they must continue to allow Merrick or its auditor to do separate examinations .

I want to conclude by reiterating our absolute commitment to data security in the card transaction and payment process. Merrick insisted upon and relied upon the CISP certification for CardSystems. When we were informed of the breach, we immediately called in expert forensic IT auditors and insisted upon immediate remediation. We are very closely monitoring the accounts of any of our potentially affected cardholders whose for unusual activity. We have been and will continue to work with our processors and Visa and MasterCard to ensure that the processing system continues to function with security, dependability and integrity. I want to again commend this Committee for its hard and good work to formulate sound public policy that will assist in achieving that goal. Thank you.