STATEMENT OF
JOHN D. MACAULAY
VICE PRESIDENT HEALTHCARE AND LIFE SCIENCES
ANAKAM, LLC
BEFORE THE
AMERICAN HEALTH INFORMATION COMMUNITY
CONFIDENTIALITY, PRIVACY, AND SECURITY WORKGROUP

September 29, 2006

Good Morning Chairman Feldman and Chairman Nahra and Members of the Workgroup. Thank you for inviting me here today to discuss our identity management and authentication work in the heath information technology field.

Benchmarking Against the Financial Industry

Let me start by saying that *we have seen the future*…and it is online banking.

- Over five hundred Phishing and other online attacks per day.
- Widespread consumer fear, lack of adoption and attrition due to privacy concerns.
- Government intervention (in the form of FFIEC Guidance) clearly stating that user name and password is not enough and that second factor authentication measures are strongly recommended.
- Banks rushing to adopt these strong authentication measures to secure consumer facing portals and protect their brands

Why do fraudsters target banking? Because that's where the users are…that is where the economies of scale exist for social engineering scams which count on luring only a small percentage of users into compliance- resulting in yields of tens or even hundreds of thousands of dollars per online attack. We believe that as PHR's and EHR's proliferate and users reach the tens of millions, fraudsters will set their sites on many of the health care sites, starting with those with the largest user bases coupled with the weakest defenses...because that is where the money is.

Further examination of the experience of the financial industry is instructive as to how organizations involved with PHR's and EHR's might avoid some of the pitfalls experienced in other areas of online commerce. While there are valuable lessons learned from the implementations in the financial industry, we fundamentally believe the challenges faced by the healthcare industry require a different approach, but potentially with similar technologies.

For example, the financial industry is able to "tolerate" a certain amount of fraud, and consequently, walks a difficult risk assessment line that balances the costs of certain security measures versus the risks of compromise. In contrast, for the health care community, breeched PHR's containing, for example, mental health, substance abuse or HIV status of users represent an entirely different level of risk to patients and practitioners- as well as the brand names and public perceived trust of the system owners. For identity management, as online fraud approaches have evolved to greater levels of complexity, the banking industry has slowly evolved from single factor authentication of simple user name and password through more complex password entropy requirements to institutional questions, and now is finally starting to implement two-factor authentication solutions. Interestingly, they have used one time pass code hard tokens for providing second factor authentication for their employees within their enterprises for the last 8-10 years. These hard token systems are time tested for security; however, these institutions also knew that issuing key chain tokens, in some cases, to millions of remote users was much too expensive and logistically cumbersome. Given this fact, some financial entities decided to issue key chain tokens to their high net worth clients. The problem with this approach is that it can send the wrong message to customers: "only the wealthy get adequate security." Such a message would be a disaster for the health care community.

In terms of Identity Proofing, until the Patriot Act amended the Banking Secrecy Act to counter the funding of terrorist activities, the financial industry did not have the ID proofing and credentialing requirements that we have in the healthcare industry. When you conducted a financial transaction online, a bank was less concerned about whether or not you are who you say you

are, and they were more concerned about whether or not you are the person who put the money in the account. Again, the banking industry has been able to change through evolution rather than revolution – they have now arrived at a point from which we might receive some benefit – the ability to have a low-touch or no-touch ID proofing transaction. Some banks have needed a mechanism to acquire customers through the Web and not require them to present themselves at a branch or office for a government-issued ID to be verified. These mechanisms are in place, and provide a model from which we can benefit in the implementation of PHRs into the future.

The financial industry has evolved to a position where strong authentication is an implicit requirement, and in many cases now, institutions are adopting two-factor authentication for appropriate controls. One final takeaway from the experiences of the financial industry is that the policy guidance should be as explicit as possible. Only when the authentication standards and concomitant policy are detailed, clear, and explicit, will industry be driven to adhere to those guidelines.

Armed with some insights from the experiences of the financial industry, now let's talk about what we believe are the elements of an identity management system that can work for the health care industry.

Multi- Layered Defense: Binding the ID Proofing Transaction with Credentialing and the Authentication Transaction

In our client, we explain how ID Proofing and Authentication are component parts which fit into the broader identity management lifecycle:

- The first component, Registration, is when the registrant provides all of the information necessary to complete the ID proofing and credentialing transaction and obtain their authentication mechanism. Registration should occur once, and then allow updates to the user's identity and profile in the future, once it is established.

- The next step, ID proofing, verifies the authenticity of the claim of identity – this depth of this process controls the risk the enterprise is willing to accept. There are some electronic implementations that simply verify that the information presented is accurate – for example with banks, they want to see if there is a person who has the name, social security number, address, and date of birth provided, but are less concerned that the person at the keyboard is actually that person. Alternatively, there are solutions, like obtaining a passport, that require one to present oneself in person at the post office, present two forms of government ID, a birth certificate,…and so on. Executed well, these face to face ID proofing applications are very effective; however, many times ID cards are forged easily and the systems fail. Fortunately, an enterprise can select from a variety of options including systems that allow electronic confirmation that the person at the keyboard is the person who's data was entered into the computer, yet it requires no face to face interaction. Designed and implemented correctly, these no touch electronic systems can be as effective, or even more effective, than in person ID proofing systems.
- The third step, Credentialing, defines attributes of the individual that will define how one's enterprise will work with them. For example, if they are a physician, a system can provide access to Physician credentials such that one's electronic business processes can be tailored to their credentials. Likewise, a patient could be credentialed as being a veteran, or a senior citizen, or eligible for Medicaid. All of these are attributes of the identity, not the identity themselves. Unlike Registration and ID Proofing which typically occur once in a business cycle, credentialing has some form of periodicity associated with it. For physicians, one can re-credential based upon the known expiration date of their prior credentials. One can also re-credential more frequently, such as in the cases of special licensure requirements for medical procedures or privileges surrounding controlled substances prescribing, based on a business need to do so.
- Next is the process of authenticating at a transactional level offering second factor authentication involving the one time delivery of a pass code to either the user's cell phone, office or home phone or email account.. The ID and credentials have been bound

to the second-factor virtual identification of the registrant and therefore ID proofing and credentialing are no longer needed unless one's business needs define the need for re-credentialing as described above. Once the authentication is completed satisfactorily, the identification and the credentials are handed off to the application to used for the business purpose.

While each component may have some vulnerability to a determined hacker, the combination of components makes fraud and breeches very unlikely. For example, a disgruntled medical staff member may be able to get through a physician automated web-based ID proofing process but it will do no good because that same staff member cannot get past a second factor authentication system at the transaction level. To accomplish the latter, the staff member would need to know the physician's user name, password, be using a pre-authorized device, and have in their possession the second factor token…collectively, very unlikely. Interestingly, under some PKI deployments, the system could be compromised quite easily (by a disgruntled staff member) if the system allowed the physician to store their private key on a particular hardware device such as an office PC. Under this PKI scenario, the system cannot tell who is behind the keyboard.

Authorization and Access Control

We understand the need for patients to have control over how information in their PHR is accessed and used. In our view of the PHR business, all medical practitioners would be able to publish and request access to the PHR. The patient would have an appropriate level of control over what data was included in the PHR and then who could view it. We support the use of the Medical Information Exchange Model which would be based upon well-defined standards such as those derived from the National Information Exchange Model (NIEM). These models all rely on a publish-and-subscribe model where access to a record within a folder is controlled by user- and role-based permissions. The folder owner (analogous to a patient) controls what elements within a folder the subscribers have access to. The publishers (analogous to providers) would publish data and request that it be included in the PHR, and when included the folder owner would specify who can see the new data in the record.

Fundamental to this approach is an effective authorization and access control system. A final element of such a system is the ability to issue an additional challenge requiring second factor authentication for anyone attempting to access a particularly sensitive portion of a PHR.

The role of government in driving policy for identity proofing and authentication

In the end, we believe that the government in concert with industry should establish the minimum standards for ID proofing, credentialing, and access control and it should be left to the system owner, the practitioner, and the patient to choose the mechanism they use to meet this standard. The government can set the minimum standard simply by referencing existing federal minimum standards for information protection – such as those found in NIST Special Publication 800-63. To be specific, we believe that the privacy and security of personal health information justifies a minimum of Level 3 controls as defined by NIST Special Publication 800-63. One difference we see is that, unlike SP 800-63, which ties those levels to the technical means used to achieve those levels, we believe the levels in the PHR space should be tied to the roles of users within the PHR user community. Finally, we wanted to underscore the importance of government and industry being proactive in developing clear standards and providing detailed and explicit policy guidance to help enforce those standards for the benefit of all stakeholders. This approach will help prevent some of the confusion and reactionary mindset that has hindered the financial industry's ability to implement appropriate systems for combating online fraud.

Potential Implementation Costs

Protecting the confidentiality, privacy, and security of patient data will come at a cost; however, systems which require no special hardware or user software help to mitigate the traditional high deployment costs of hard token based systems.

Interestingly, while the increased costs of security may seem like a barrier, they are also an enabler for success. With increased security, system function and depth of information becomes

richer; this has a direct impact on driving user adoption – particularly adoption by physicians. With increased adoption by physicians, we will see a commensurate increase in adoption by consumers which will, in-turn drive unit costs down. At the same time, the value of the aggregate data helps sustain the price point since, with more participation, the dataset and function becomes more valuable. As has been seen on numerous medical information portals, participation in the system by physicians drives user adoption and participation. If the doctors don't participate, the patients won't either.

Summary

In summary, we believe that in order to accommodate what could be a very fast adoption rate of HIT in general in the next few years, security systems for PHR's and EHR's should have the following characteristics:

- Be based on detailed standards jointly developed by government and industry.
- Allow no touch ID proofing upon enrollment
- Allow electronic credentialing of physicians and other medical practitioners using only the most trusted credentialing data sources
- Require second factor authentication that can be repeated within an application for added security while accessing the most sensitive areas within a PHR or EHR.
- Provide a real time fraud alert to patients and practitioners should a fraudster be trying to access a PHR or EHR.
- Be scalable and affordable by using hardware that is ubiquitous in the health care environment.
- Rely on an easy and intuitive user interface and require no software downloads for patients or practitioners.
- Provide technical non-repudiation, data integrity and customizable reporting for HIPAA/CLIA and other regulatory compliance requirements.

Chairman Feldman and Chairman Nahra and Members of the CPS Workgroup , as a company, like many other fine companies in this space, we are excited to be in a position to contribute in our own small way to the future success of PHR's and EHR's. Working together, we all can contribute to developing a PHR which contains comprehensive patient information, available 24/7, fully endorsed by physicians, linked to relevant resources and secured by identity management systems which fully protect the most important element of all: public trust.

This completes my statement. I'll be happy to answer questions during that period on the agenda.