

## IN THIS ISSUE:

- ≡ Preventing Cyber and Electronic Related Losses
- ≡ Smart Phones: The Next Cyber Crime Frontier

## Preventing Cyber and Electronic Related Losses

**Much attention has been given to a recent lawsuit between Comerica Bank and their treasury management client, Experi-Metal. Conduct an Internet search and you will find numerous articles about the suit and its merits. The following briefly recounts the criminal event and subsequent lawsuit:**

Experi-Metal fell victim to a phishing attack that led to 93 fraudulent payment orders executed in 6 1/2 hours totaling \$1.9 million. The majority of the funds were siphoned from one of the company's Comerica accounts to accounts world-wide, including Russia and Estonia. Comerica was able to recover all but \$560,000. Experi-Metal subsequently sued Comerica to recoup the unrecovered stolen funds, claiming Comerica did not act in good faith. Comerica countered that they followed all applicable banking regulations and law. A bench opinion ultimately ruled in favor of Experi-Metal, finding that Comerica did not act in good faith with respect to the incident.

While the legal merits of the suit are well beyond the scope of this article, a broad examination of how insurance coverage responds to Internet, cyber and electronic-related claims is a valuable exercise as incidents of unauthorized access, customer hacks and data breaches continue to increase.

Electronic-related crimes began even before the World Wide Web existed—corporate and bank networks were hacked via phone lines.

Article continued on next page ⇨

## Smart Phones: The Next Cyber Crime Frontier

By John Jaser, Internet Services Manager, COCC

**A few years ago, a colleague showed me an idea for a movie thriller where computer hackers take control of a neighborhood's PCs, smart phones, thermostats, toasters, cars, even pacemakers to extort money from helpless residents. Today, my colleague's movie idea could be playing in any neighborhood in the United States.**

He's not looking for royalties. **As a matter of fact, we both wish the idea remained a matinee fantasy, not an emerging cyber crime reality.**

Article continued on next page ⇨

## SIDE NOTES

### ABA Insurance Risk Management Forum

Date: January 22 - 25, 2012

Place: Loews Miami Beach, Miami, FL

**It's time to mark your calendar for the industry's leading insurance event, the ABA Insurance Risk Management Forum.**

### *Real Life Solutions for Risk Management's Complex Challenges*

In a world increasingly dominated by the extreme, the unknown, and the improbable, the ABA Insurance Risk Management Forum ([www.aba.com/Events/IRM](http://www.aba.com/Events/IRM)) is your reliable, go-to source to prevent liability exposures from catching you by surprise.

Gain executive insights from top insurance risk managers on where the industry is heading. Examine new types of protection against data center losses, social media, mobile banking, and other evolving risks. Gain in-depth expertise, case studies, and resources on how to limit your exposures and be better prepared for risk management's new normal.

Hear expert keynote speakers discuss what regulatory changes and interlinked global economy mean for your risk management operations.

**Preliminary program information now online:**  
[www.aba.com/Events/IRM](http://www.aba.com/Events/IRM)

**To Register**, visit [www.aba.com/Events/IRM](http://www.aba.com/Events/IRM) and click "Register Online" or call the ABA at 800-BANKERS.

### MEMBERSHIP REMINDER

The American Bankers Association has begun their 2011-2012 Membership year. Don't forget to renew your membership! *Not a member?* If you purchase your bank's coverage from ABA Insurance Services and are an ABA Member, you are automatically a shareholder in the program's mutual reinsurer, American Bankers Mutual Insurance, Ltd. Your bank is then eligible to share in the program's success. To date, this unique distribution program has declared \$75.5 million in profit-sharing over 21 consecutive years. Contact Karen Call at 800-BANKERS or [kcall@aba.com](mailto:kcall@aba.com) to renew your membership or join the ABA.

---

## ■ Preventing Cyber and Electronic Related Losses, *continued*

With the rise of the Internet came the increase and scope of criminal activities. While each scam has a different nuance, the ultimate goal is the same—trick a user into surrendering personal and confidential information, such as social security numbers, account numbers, login IDs, passwords, etc., which the perpetrator can then use to commit financial crimes.

Obviously, specific facts and circumstances of a claim determine where coverage may or may not be afforded. However, when an electronic-related loss occurs, insurance companies generally refer to:

1. Computer or Electronic Crime coverage to indemnify the bank for financial loss, and
2. Internet banking liability policies to determine if the insured is legally obligated to pay for the loss.

**Internet Banking Liability or Cyber policies** are written to cover judgments, settlements and defense costs stemming from wrongful acts that the bank or an employee is legally obligated to pay. These claims often involve:

- ≡ Invasion of privacy (the failure to protect confidential customer information),
- ≡ Unauthorized access to a customer account, and
- ≡ Copyright or trademark infringement.

First introduced to the market almost a decade ago, these policies are now commonly purchased and are a must for banks with transactional Web sites.

In addition, most banks carry electronic and computer crime coverage as part of their financial institution bond. Generally speaking, the insurance is designed to make the bank whole for fraudulent transfers (i.e. wire, electronic funds, and ACH) when a bank employee acts in good faith and is reliant upon bogus instructions.

Coverage is also written to cover losses resulting from an unauthorized party, such as a hacker, entering a computer system and transferring funds. **It is absolutely critical that your bond contains a Computer/Electronic Crime Rider.**

However, be aware that this **coverage only responds when the bank's computer system is hacked and *NOT* when a customer's system is compromised.** Insurers do not cover losses resulting from a customer's failure to safeguard their passwords, deploy firewalls, antivirus or malware software, or prevent unauthorized downloads.

### What steps can a bank take to prevent such losses?

- ≡ **Strictly follow a call-back procedure to verify the authenticity of the transfer request.** Not only is this a best practice, most insurers require a call back once the transfer amount exceeds a certain threshold as a precedent to coverage. Often, a written agreement which authorizes the bank to act upon voice, email or fax requests is required as well.
- ≡ **Monitor international requests extremely closely.** It's no surprise that fraudulent requests are often directed to foreign countries.
- ≡ **Encourage your staff and your commercial customers to be alert for suspicious or unusual activity.** Requested transactions which do not fit the history of the account should raise red flags. In the Experi-Metal case, they had very limited prior wire transfer activity, yet suddenly had a flurry of 97 payment orders within a 6 1/2 hour period.
- ≡ **A frontline employee's gut feeling is often correct.** Staff should be trained to be proactive and recognize signs of possible criminal acts. Questionable activity should be reported immediately to a supervisor and actions taken in order to help prevent potential financial loss to your bank and your customers.

---

For more loss control information or to view this SafeTalk newsletter online, visit [abais.com](http://abais.com). To subscribe to SafeTalk®, request reprints, or should you have additional questions about this newsletter or its articles, please contact us at [marketing@abais.com](mailto:marketing@abais.com) or 1-800-274-5222.

## ■ Smart Phones: The Next Cyber Crime Frontier, *continued*

Apple's acclaimed iPhone was hacked within hours of its initial release in June, 2007. Fast forward to June, 2010, and we see Apple still battling iPhone security issues. A new release of the iPhone mobile operating system closed 65 vulnerabilities. More security measures were required to prevent consumer account breaches in Apple's online iTunes store. An ongoing problem with iPhone 'data leaks' is still unsolved.

The iPhone's popular cousin, "Droid" by Google and Motorola, reportedly has similar security issues. Back in December, 2009, we heard reports of criminals gaining control of other users' Android 2.0 or Android 2.0.1 version phones.

Apparently, the criminals are lacing free smart phone applications with their own code to attack users' phones. The users download the free applications and get a lot more than they bargained for. It's an old infection technique honed from PC days, but smart phones raise the risks to an entirely different level.

You see, every smart phone has "gadgets" such as a camera, microphone and geo-location service (GPS). When infected, the smart phone's gadgets can be controlled by criminals who can literally track the user's location, such as when the user enters a sensitive facility. The criminals can then activate the smart phone's camera and microphone, giving them eyes and ears where the user wants them least.

Couple this type of exploit with a growing smart phone "botnet" (thousands of hacked smart phones operating under the control of criminals) and we are looking at a thriller beyond Hollywood proportions. More ominous, the code to do this has been published on the web for other criminals to review, refine and reuse.

Apparently, the criminals have wasted little time. In January, 2010, Google removed nearly 50 applications from its Android Market in response to concerns that they might be malicious. The applications offered access to

bank accounts at JPMorgan Chase, HSBC, and ING. At least one of the applications was infected with an exploit designed to steal the user's bank login credentials.

This has not stopped Bank of America, TD Bank and USAA from forging ahead with their own Android-friendly mobile applications. Chase Bank recently added remote deposit capture and peer-to-peer (P2P) payments to its iPhone application. I can't imagine that other banks won't follow suit, with early adopter customers not far behind.

Certainly, we are heading into a 'Gold Rush' for killer smart phone banking apps, and just as certainly, the criminals are watching every move with cunning, guile and greed. After our experiences with phishing, botnets and other debilitating attacks on the Internet banking channel, we should be smarter about preventing criminal activity on smart phones.

Smart phones are essentially online laptop computers equipped with GPS and hundreds of third party applications. Banks need to regard smart phones as untrusted platforms since they don't know what the user has installed or subverted, intentionally or not.

All of this screams "opportunity" to the security application community, and sure enough, solutions such as Lookout have already attracted one million users, according to the technology weblog TechCrunch. Norton, Kaspersky, Trend Micro and F-Secure are now peddling their smart phone security solutions as well.

The challenge for banks is to ensure that their mobile banking customers have installed and are using security solutions on their smart phones. Applications do exist for this purpose, and banks would do well to deny transactions from customers who aren't protected.

Marketing might howl and customers might threaten, but banks should remind them that criminally-controlled smart phones are not in their best interest, except, of course, in a movie theater on the big silver screen.

**About COCC:** COCC delivers complete enterprise processing solutions to banks throughout the northeastern United States. Listed among American Banker's FinTech 100, this client-owned technology company has a history of implementing leading edge technologies. COCC has been recognized for superior client service and advanced technology, particularly for its work in data security, desktop and server virtualization, solid state disk storage, and SaaS implementations. Client ownership make COCC the better data processor. For more information, please visit [www.cocc.com](http://www.cocc.com) or follow on Twitter @coccinsight.

© COCC Financial Technology Solutions. White Paper, reprinted by permission.