Welcome & Opening Remarks
JBA President Maureen Hayden-Cater
JIFS/JBA Anti-Fraud Seminar
Terra Nova Hotel
September 10, 2014

Salutations

The issue of fraud continues to be a contentious and on-going matter of concern both for the banking sector and the customers we serve.

Specifically, we are faced with three types of fraud in Jamaica: cheque, card and internet fraud, with the latter two having grown substantially in scope and practice, and alarmingly so, over the last decade. This is as a direct result of the increasing use of technology, which has not only made businesses more efficient, but unfortunately has also provided fraudsters with a more efficient tool.

As an example, card skimming and cloning entered Jamaica's business environment around 2002 and since then, it has experienced peaks and troughs, with the peaks occurring at or near a major spending period. The latest peak has deviated from that norm, as it started in February of this year and continues even now. Hopefully this is not a new trend, which would mean that it will be a more constant threat.

Meanwhile internet fraud has logically risen with the growth of internet banking. Unfortunately, our local fraudsters have gravitated towards it as a new and, unbelievably, “safe” source of income.

The repercussions of fraud are of course, varied and wide in scope, with the main effect being a loss of revenue, and increased security costs. Just

think: cash can be stolen with just a click of a mouse. Another effect too is the time that is wasted when IT personnel must devote great portions of their day handling such incidences.

Just this week (September 9, 2014) Home Depot reported that it has uncovered a major fraud where credit card information for 60 million of its customers had been accessed by hackers, and what was even more frightening is that they had been in the system for a while, unnoticed, until someone came upon a transaction in cyberspace and reported it. Prior to this, the largest such case was a few months ago when Target similarly reported that the credit card information for 40 million customers was accessed.

A bank's reputation can also take a major hit, such as Home Depot and Target mentioned before. Customers whose credit card or other financial data become intercepted by hackers for example, may lose confidence in an organization and often begin taking their business elsewhere. Such vulnerability can lead to a decrease in the market value of the bank, due to legitimate concerns of financial analysts, investors, and creditors, through share price reduction.

This, as implied before, is a global trend, and we are not alone in Jamaica. If you take a look at the emerging threats in the global marketplace – a topic that will be discussed a little later on today – you'll see that along with these three fraud types, there are a myriad of new challenges that come up almost daily.

But what seems to be the most urgent issue comes from the growth of mobile banking. Globally, millions of consumers are already using a wide array of mobile devices to conduct banking; millions more are expected to go mobile in the coming years. But with that growth comes a whole new set of threats, which we must be prepared for:

- Mobile Malware - These include trojans and viruses migrating from traditional online banking and designed specifically for the mobile marketplace. Researchers see an increase in mobile malware development, which is in pace with market growth.

- Third-Party Apps - Consumers love their smart phone and tablet applications, but often these apps come from third parties with sometimes questionable security practices.

- Unsecured Wi-Fi - The unsecured wireless network is an easy highway for fraudsters to gain access to mobile devices, either to seize control of, or gain access to account information.

- User Behavior - Consumers are prone to download third-party apps, use unsecured wireless networks, open and click links in SMS text messages and e-mails, and lose their mobile devices. Mobile-use behavior is creating a suite of vulnerabilities, and fraudsters are eager to take advantage.

Much of this comes from the industry's reliance on third party systems to provide many of their digital services. Whether it is external data feeds, customer and staff devices or cloud services, banks find themselves having to rely on systems that are outside of their control. And importantly, should a problem occur, the banks own all the risks, not the third party providers.

This is a major concern as more persons add data plans to their phones here in Jamaica, with the PIOJ pointing out that at the end of last year there were 780,000 data subscribers, and more banks promote the use of internet banking, inevitably, we will see more problems arise in this arena.

What can the JBA do to combat these and other fraud practices? Some of the measures we have implemented over the years include: staff training and customer education; strict privacy policies; rigorous security and encryption systems; constant upgrading of ATM, credit card and online account security; video surveillance at branches and ATMs; monitoring of account activity to identify suspicious or unusual transactions; dedicated resources for investigation of fraud cases; and prosecution of criminals.

We've also instituted these seminars in an effort to keep you the members of the banking industry adequately informed on new and current fraud practices.

Most importantly, just as with personal security, at the home or office, the most important thing is to be aware of the possibility of threats and be vigilant about reporting and combating any suspicion. We are always most vulnerable when we let our guard down, and therefore it is crucial that we remain aware.

We must also be aware that there are significant cost implications if we fall prey to these schemes, and so we should not compromise our efforts and resources in trying to prevent them from happening.

Without a doubt, our speakers for today will also provide additional ideas and mechanisms through which we can tackle the issue of fraud within our industry, without placing constraints on business innovation and growth, and I am hopeful that those of us in attendance will put these suggestions to good use.

The JBA will no doubt play a critical role in educating our members and public about these threats, and ways in which we can prevent them.

Maureen Hayden-Cater
President
Jamaica Bankers Association

September 10, 2014