CISBC/YT Financial Crime Awareness Bulletin

January 30, 2010

UNCLASSIFIED
(Public Version)

Inside this issue:

RFID stands for **Radio-Frequency IDentification**.

The acronym refers to small electronic devices that consist of a small chip and an antenna. The RFID device serves the same purpose as a bar code or for our purposes, the magnetic strip of a credit or debit card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information. *(www.technovelgy.com)*

RFID Technology in Payment Cards

A US based news video regarding RFID technology and the concern over "electronic pickpocketing" recently circulated. Together, with a CBC news article from June 2010 regarding the technology, it caused speculation as to the validity of this as a fraud concern. Was the video clip just hyped up because a private company promoting their protective sleeves to shield these cards from potential skimming devices was featured?

The purpose of this bulletin is to address the above by explaining the "**R**adio **F**requency **ID**entification" technology (RFID) that has been implemented in credit cards in Canada.

This relatively new feature of "contactless payment" aka "Touch and Go", "Wave and Pay", has been introduced by the payment card industry as a "secure and convenient" enhancement to expedite our daily financial transactions. Mastercard's PayPass will be 100% RFID enabled on their credit cards this year as they started in 2006 and VISA is continuing it's implementation of payWave.

However, with this also comes the potential for more fraudulent criminal activity. This bulletin was initially produced for fraud investigators but has been sanitized down to this version in order to raise awareness with the general public as we all inevitably use payment cards in some way or another.

RFID symbol on cards

This public version of the bulletin is a compilation of both open source information and subject matter expert responses over fraud risks and privacy issues.

"electronic pickpocketing" video link:

http://www.wreg.com/videobeta/?watchId=8ba6f8fc-90a2-4711-90ea-1884ec348310)

How RFID works and Why do we have it?

The embedded chip and antenna enable consumers to wave their card over a reader at the point of sale. Because no swiping or signature is required for low limit transactions, it can be almost twice as fast as a conventional cash, credit, or debit card purchase. Basically it's "what the consumers wants, is what the consumers gets" - convenience.

It appears not only to be advantageous for consumers, but also for merchants and banks. Some studies have indicated that consumers are likely to spend more money due to the ease of small transactions hence the push towards RFID.

MasterCard: Aims to have all cards in Canada enabled with its PayPass contactless system by end of year.

MasterCard Canada says it has seen "about 25 percent" higher spending by users of its PayPass-brand RFID credit cards.

(Dubinsky, Zach. "New credit cards pose security problem" CBCNews.ca 2010-06-02).

Global View

Major financial entities across the world now offering contactless payment systems include MasterCard, Citibank, JPMorgan Chase, American Express, KeyBank, Barclays, Barclaycard and HSBC. Visa payWave and Mastercard PayPass are examples of contactless credit cards which are widespread in US, UK and now Canada. Since its introduction in 2004, Visa payWave has provided cardholders around the world with a faster and more convenient form of payment than using cash and checks.

The UK (and the rest of the world) version of the contactless applications has the capability of transacting remotely, based on the limit stored in the application unlike the North American one which has no power source of their own so card data cannot easily be accessed remotely .

Canada

RFID credit cards surfaced in Canada in 2006 when MasterCard started aggressively pushing its PayPass cards. Today, about 90 per cent of MasterCards in the country are RFID-enabled and the company aims for 100 per cent by the end of 2010, said Scott Lapstra, vice-president of market development for MasterCard Canada.

MasterCard PayPass

Visa has been slower to market such "proximity cards" under its own brand, payWave in Canada. Royal Bank decided only this year (2010) to make all its Visas payWave-enabled and all newly issued TD Visa cards have the feature. But most Visa cards in Canada, including those from CIBC and Scotiabank, don't have RFID. Both Mastercard and Visa limit contactless purchases to $50 each and have pushed to have reader terminals installed mainly in high-volume, low-price businesses like big-chain coffee shops, fast-food outlets, gas stations and grocery stores.

Dubinsky, Zach. "New credit cards pose security problem" CBCNews.ca 2010-06-02.

Credit Cards

The RFID transactions in Canada are based on the international EMV chip standard which provides the most advanced and widely adopted cryptographic security for payments today. They are designed to offer cardholders speed and convenience, most of the time cardholders will not need to sign or enter a PIN to complete a low limit transaction.

Any debit or credit card with this logo is RFID enabled:

"Contactless" MasterCards and Visa cards have been available in Canada for several years, but they've only recently reached the bulk of consumers as the country's biggest banks adopt them. Recent media reports surfaced due to the concern of how secure this technology is and the potential fraud risks we may be facing in the future. Videos demonstrating how easy it is to 1) acquire an RFID card reader (via eBay, Craigslist, etc.), 2) get into close proximity with anyone in public and 3) scan for personal unencrypted information embedded in the RFID cards, are raising the issues.

Credit Cards—Pros and Cons

Credit card companies are claiming the following advantages for contactless credit cards:

- card is faster to use - faster, convenient and less fumbling for cash
- cards use high secure data transmission standards
- Merchants can cut down on lineups which boosts average sales...studies show the average "spend" rose fifteen percent for all contactless credit card users.
- Safer and more secure because the card does not need to leave your possession

The following disadvantages have been noted with contactless credit cards:

- A thief armed with a suitable reader, would be able to skim unencrypted data such as card number and expiry date and in the first generation RFID cards, the cardholder's name. Although they can't duplicate the card for purchases with this limited information, it could be used to commit ID fraud.
- Privacy advocates are particularly concerned about this technology; it is feared that having this much information available "in the open air" will lead inevitably to problems.

VISA Canada, also responded to this issue and the following is a sanitized excerpt of what was disseminated to fraud investigators across the country:

"Ensuring payment security is one of Visa's highest priorities. Visa payWave cards meet all of the same standards of security used in traditional card payments. All Visa contactless transactions are based on the international EMV chip standard which provides the most advanced and widely adopted cryptographic security for payments today.

Security features found on every Visa payWave card include short read range and an encrypted code that is unique to a particular transaction and changes every time the card is used. This is known as dynamic card authentication and ensures that stolen card information is useless and cannot be used to create counterfeit cards or to make fraudulent transactions.

In addition, Visa has safeguards to protect personal information. Minimal account information is stored on contactless cards, which is similar to the traditional security features on magnetic stripe cards or contact chip cards. In fact, newly issued Visa payWave cards do not even transmit the cardholder's name during a transaction.

Q: Can someone with a card reader stand close enough to a cardholder to steal the account or card information from a contactless card without the cardholder's knowledge?

Yes, but the individual would need to get very close and would need to know the location of the cardholder's card.

Further, only minimal account and information is stored on a Visa payWave card, which is less than traditional magnetic stripe cards or contact chip cards.

The account information contained in a contactless payment card or device contains the same minimal personal information currently found on a traditional magnetic-stripe card or chip. Contactless transactions are processed through the VisaNet system exactly the same way as traditional cards and enjoy the same level of security protections and fraud prevention.

Further, Visa payWave cardholders are protected by Visa's multiple layers of security, including Verified by Visa, CVV2, Address Verification Service (AVS), Visa's neural networks, Visa's E-Promise and Visa's Zero Liability policy, which protects all Visa cardholders from unauthorized purchases."

Debit Cards

INTERAC Association confirmed that there are currently no RFID debit cards in Canada. However in the near future, Interac Flash will be introduced as the new contactless enhancement of Interac Direct Payment.

INTERAC was contacted in regards to RFID and debit cards in Canada, and the following comments were put together for this public bulletin on 2010-01-20 on "Electronic Pick Pocket":

"Issue

There have been some media stories in the United States indicating that fraudsters can steal card data from contactless enabled credit and debit cards using a small computer device positioned near the wallet/card.

Message

INTERAC debit cards are protected from the "electronic pick pocket" fraud tactic. In addition, the new INTERAC Flash contactless enhancement of INTERAC Debit is also protected against this fraud tactic. INTERAC Flash leverages EMV chip security. The con tactless transactions in the US tend not to leverage these standards. In addition, INTERAC Flash leverages RF enabled smart card technology, which is designed to protect sensitive infor mation and adheres to an ISO standard 14443. We do not use RFID technology. Finally, the IN TERAC system does not allow for card-not-present transactions. Further, given the structure of INTERAC Online, stolen cards and even PINs cannot be used to complete Internet transactions."

Liability

Contactless debit and credit transactions continue to be protected by the same fraud guarantee as standard transactions, i.e. financial institutions claim to be liable for any fraudulent transactions charged to the contactless cards.

However, banks are not liable for the identity theft that the RFID card can encourage.

A number of products are available on the market that will allow a concerned carrier of RFID-enabled cards or passports to shield their data. The most popular one used would be the protective sleeve that encases the card.

It is a legitimate concern since recently, even UK RFID enabled passports were compromised. In 2008, cross-border

Visa: Has 31 million cardholders in Canada but would only disclose that "several million" of those contain its payWave RFID technology. Major issuers are Royal Bank and TD. Notable non-players are CIBC and Scotiabank

RFID enabled NEXUS passes were re-issued with the added protective card sleeves and an awareness notice.

CISBC/YT
Financial Crime Portfolio

Comments and suggestions are welcome for future publications. We acknowledge CISBC/YT partner agencies that have contributed to this bulletin.

CISBC/YT Phone: 604-264-2727

Promoting inter-agency co-operation within our BC Law Enforcement community

www.cisc.gc.ca/cisbc-yt

The mandate of **CISBC/YT** is to be a strategically-focused organization which ensures the timely production and exchange of criminal information and intelligence among CISBC/YT member agencies. It shall provide facilities for the collection, analysis and dissemination of significant criminal intelligence to aid in combating the spread of organized crime in British Columbia, Yukon Territory and Canada.

The **Financial Crime Portfolio** is responsible for reporting on the activities seen in BC/YT within this criminal market as it pertains to Organized Crime. Intel is gathered from all financial crime sections in law enforcement as well as Category II agencies that deal in this area... CBA, FINTRAC, CRA, BCSC, Canada Post and GPEB to name a few.

Please contact the bureau should you wish to share any information with us.

Remarks

It appears that the main issue is that these RFID cards are openly susceptible to criminals who can skim for information that is not encrypted by using readily available card readers. The credit card number, the expiry date, and in the first generation RFID cards, the cardholder's name, are not encrypted by the credit card companies.

It is true that with only this information at hand, no counterfeit cards or purchases can be made - i.e. fraudulent purchases cannot be made in person or in cards-not-present situations (over the phone or internet as they still require the 3-digit security code from the back of the card that can't be acquired via the card reader).

However, it does mean that cardholder information can be easily obtained without the card being physically taken from the cardholder. This means that there is more of a chance for Identity theft which always is followed by Identity Fraud. With this initial information from the cardholder, one can then acquire more information from the victim by calling them up ("spoof calls"), impersonating the bank and asking for them to "confirm" the security digits on the back of their card.

Potential ease of skimming data

The Canadian Bankers Association has mentioned that they have seen an increase in these types of spoofing calls this year. This trend is exactly the same as what the United Kingdom had experienced with the introduction of RFID cards a few years earlier.

In conclusion, although the potential is there for individual skimming, the current debit skimming techniques and point of sale terminal thefts used by the criminals allow them access thousands of payment cards in a shorter time. Therefore, the older MO's are still more profitable and feasible than RFID skimming from one individual at a time, but that doesn't mean they won't be utilizing this method, so STAY AWARE!