Inside Cash Management NEWSLETTER

NOVEMBER 2018/Issue 8

CIBC FirstCaribbean International Bank

IN THIS EDITION

Online Banking - the meeting place for CIBC FirstCaribbean clients

This year, CIBC FirstCaribbean received the award of "Most Innovative Bank" in the region from United Kingdom-based World Finance magazine. We believe in leveraging technology to constantly innovate and deliver the best client experience.

Using online banking helps you save time and money. It's like having a branch that's open 24 hours a day, seven days a week. Apart from using cards, a major percentage of customers use their online banking accounts to transact online. Online banking transactions contribute to a significant amount of the overall traffic across the internet globally, thereby making it an important mode of payment and collection.

Check your accounts and carry out transactions whenever it suits you. That way, you can focus on what matters most according to your daily routine. Using electronic statements can help with seamless integration with popular accounting systems to reduce the need for manual processes.

It's easy to pay your employees via the Internet. You can also send funds directly to other businesses such as suppliers or utility payments. The integrated Online Bill Payment module allows you to make payments to a pre-determined list of billers directly. Our Online Banking Solution for businesses facilitates foreign currency transactions (buying and selling during business hours).

Most importantly, this solution uses multiple layers of security such as RSA SecureID tokens to ensure the secure transfer of funds, Controls for the Segregation of Duties to ensure that officers who authorize transactions are separate from Officers who initiate the same transaction. Your business will have total control over the access privileges granted to employees who use the service. Our multi-user platform provides for an Administrator profile which is designed to manage user profiles. User profiles can interact and transact on the accounts that have been specified by your company's Administrator.

When you bank online with CIBC FirstCaribbean, your security is our primary concern. When you Log on to your accounts, your confidential account information is protected by one of the most secure forms of encryption widely available for Internet browsers. Please feel free to see more details by clicking: here.

A truly secure banking environment is a partnership between you and your bank.

Requirements;

1. Completed Corporate Internet Banking Registration Form
2. Access to the Internet and a Computer

Next Steps: Contact your Relationship Manager or Cash Management Sales Officer for further details and forms.

Editor's Note

Our fiscal year draws to a close at the end of October, but at CIBC FirstCaribbean we are just getting started!

Our intention is clear - to remain at the forefront of innovation, leveraging our strong technology base to guarantee that your enterprise stays current with improvements that will continue to revolutionize the service you provide to your clients.

This edition continues to set that pace.

Our teams examine the risks and threats of fraudsters to successful commerce; the techniques they use to illegally garner information, for example, at point of sale terminals; and the role of business leaders and employees in maintaining vigilance to prevent unwarranted attacks. We encourage you to take advantage of the helpful tips provided.

If you are not already taking advantage of the myriad benefits of our online banking solutions for corporate clients, this edition takes you into the world of our unique online banking platform that provides the added value and security you need to run your business more efficiently. Always wanted to know about our Electronic or E-statement product? This edition also takes care of that!

There's much more to digest and our team of experts continues to enjoy sharing their knowledge with you. As always we are a phone call or an email away to hear your views and suggestions for making this publication the best it can be.

Enjoy!

Andre Delgado
Associate Director, Cash Management & Trade Finance

Point of Sale (POS) Terminal Attacks – What you need to know!

Attacks on businesses by fraudsters are frequent and creative. Wherever there is commerce and a means of passing value, you can be sure that there will be a risk of exposure to someone who is willing to exploit any vulnerability to their own benefit.

Point of Sale (POS) terminals, while having a higher level of security by virtue of the transactions being completed in plain sight and with the interaction of the business' representatives, do pose some risk of exposure if adequate security measures are not observed. There is growing awareness of the tactics and technology used by fraudsters in perpetrating POS skimming attacks.

The Targets

While any card reader can be subject to tampering, there is notable difference in the targets chosen by fraudsters. Larger organisations or those with high velocity transactions tend to have a higher security surveillance environment and as such, will not be as exposed to some of the inherent vulnerabilities that exist with medium and small businesses using POS. As a result, smaller entities are seen as soft targets which can be used to gather cardholder data in an unsuspecting way.

The Modus Operandi

Easy targets

- Locations with lax security practices:
- Little to no surveillance
- POS terminals left unattended
- Inattentive or distracted staff

Fraudster techniques
To create a distraction or opportunity to be isolated with the terminal
Alter the existing device in some way – e.g. use of overlays or other card reader skimming devices placed on the POS
Replacement of the PIN pad with their own
Damaging the chip reader to force use of the magnetic strip reader for transaction completion

The Solution

1. Training of POS users to look for any evidence of tampering and being attentive to checkout spaces while keeping them highly visible at all times reduce the risk of exposure.
2. Immediate reporting of any attempts or incidents of POS tampering to your financial services provider and law enforcement will allow for rapid response to fix any issues identified and possibly intercept the perpetrators. No attempts should be made by the business to return the affected POS to its original state.

While it will be challenging to keep ahead of new methods and technology use to perpetrate fraud, a disciplined and collective effort by merchants, cardholders, financial institutions and law enforcement will have a profound impact on reducing opportunities and losses due to fraudulent activity.

Cyber Security Awareness against Threats

Did you know that 66% of small businesses rely on the Internet, but only 23% have an internet security policy[1]? Cyber Security is now a Business Risk; this threat has become more than an IT problem. Cyber Threats are defined as the possibility of a malicious attempt to damage or disrupt a computer network or system.

Protecting your business's interests against vulnerabilities such as phishing, unpatched software and advanced persistent threats[2], requires that you re-assess your existing infrastructure to implement security and safety precautions as this can impact its future viability.

Managing cyber security as a business risk is not as scary as it sounds. Developing simple guidelines can help your business. How can this be done? You need to develop an approach which integrates cyber protection into all aspects of the organization, from the IT department, to employee training to security policies.

The following does not represent a comprehensive list, however some areas to consider for a cyber-security policy for your business include:

1. Identifying the potential for exposure within existing infrastructure to cyber threats
2. Developing policies, procedures and oversight processes to prevent being exposed
3. Protecting your company's network infrastructure
4. Identifying and addressing risks associated with remote access to client information and funds transfer requests
5. Defining and handling risks associated with vendors and other third parties
6. Detecting unauthorized activity
7. Providing training and building awareness with employees are critical to your company's safety.
8. developing a business continuity/recovery plan (BCP). Being prepared for a security attack means knowing what to do to minimize the damage if a breach occurs.

Esan Peters, our Chief Information Officer and Managing Director for Technology & Operations reiterates that both consumers and businesses need to practice increased online awareness and maintain resilience in the face of evolving cyber threats.

"Cyber Security is about more than maintaining strong passwords and safeguarding your PIN. Each of us plays a role in keeping ourselves, our businesses and our clients safe. It's our responsibility to make sure we are up-to-date with the latest cyber criminal tactics, and the steps we can take to help prevent them from being successful."

1. *https://www.cisecurity.org/blog/october-national-cybersecurity-awareness-month/*
2. *https://www.secureworks.com/blog/cyber-threat-basics*

CIBC FirstCaribbean E-Statement Solution

The Corporate Internet banking platform provides an electronic option to bank when it is convenient. This includes viewing your accounts, facilitating payments to your employees and suppliers, and paying utility bills 24 hours a day and 7 days per week. Among the list of features, users can also view electronic statements using the prescribed format of the platform.

What if the prescribed format precludes integration with your software system which is designed to integrate with functional areas of the business?

CIBC FirstCaribbean's Electronic Statement allows greater flexibility in viewing the activity of your FirstCaribbean accounts by providing standard electronic statement reports compatible with major accounting and multibank software. The E-Statement is available either as a SWIFT MT940 statement message or an Electronic File which can be made available in a downloadable format for easy integration with popular accounting systems.

What is an Electronic file statement?

Major Accounting systems allow you to import bank and credit card statements from your Bank's platform in various formats. CIBC FirstCaribbean supports the .csv format. Electronic file statements help companies export a high volume of data to a more centralized concentrated database for ease of management. Your accounting system must be able to import .csv electronic files.

What is SWIFT MT940?

The SWIFT MT940 is a detailed statement of your account, mandated to contain a start and closing balance with all payments within (if any). SWIFT clients will receive their bank statement via a standard message. This message is called MT940. The message is sent using the SWIFT system. SWIFT was created to be a shared worldwide financial messaging service with a common language used for international financial messaging. CIBC FirstCaribbean will create and send an MT940 to the designated SWIFT address of your recipient bank or Corporate SWIFT Address, which will receive and display your CIBC FirstCaribbean account details using their platform interface. You will need to complete an E-Statement Request Form and your bank or financial institution must be able to receive and display MT940s via SWIFT.

Next Steps: Contact your Relationship Manager or Cash Management Sales Officer for further details and forms.

INSIDE CASH MANAGEMENT EDITORIAL TEAM

Fay Brandon	Corporate Communications
Samuel Brathwaite	Marketing
Andre Delgado	Cash Management & Trade Finance
Laura-Lynn Lawrence	Cash Management & Merchant Services
Carlos Moore	Cash Management & Merchant Services
Alliecia Rhone	Cash Management Sales Specialist
Damien Simon	Cash Management Sales Specialist

Talk To Us

YOUR REGIONAL CASH MANAGEMENT SERVICES TEAM:

COUNTRY	CONTACT	ROLE	OFFICE TEL.	MOBILE TEL.
Antigua	Lennox Thomas	Cash Management Sales Specialist	268-480-5059	268-464-7897
The Bahamas	Maurice Rolle	Manager Sales, Cash Management and Merchant Services	242-302-6074	242-424-8483
	Deidre Penn	Cash Management Sales Specialist	242-394-9919	242-424-1231
	Vanda Miller	Cash Management Sales Specialist	242-394-9922	242-424-7053
Barbados	Carlos Moore	Manager Sales, Cash Management and Merchant Services	246-467-8847	246-243-9235
	Carlos Bignall	Cash Management Sales Specialist	246-467-1942	246-231-0272
	Keisha Jordan	Cash Management Sales Specialist	246-467-1556	246-243-6583
BVI	Michael Jefferson	Cash Management Sales Specialist	284-852-9950	
Cayman	Bruce Sigsworth	Manager Sales, Cash Management and Merchant Services	345-815-2232	345-916-3255
	Alliecia Rhone	Cash Management Sales Specialist	345-815-2237	345-938-3305
Curaçao/Aruba	Genera Villanueva	Cash Management Sales Specialist	599-433-8218	599-670-007
Dominica	Lennox Thomas	Cash Management Sales Specialist	268-480-5059	268-464-7897
Grenada	Kasha Ragbersingh	Manager Sales, Cash Management and Merchant Services	473-437-4027	473-409-3416
St. Kitts	Kasha Ragbersingh	Manager Sales, Cash Management and Merchant Services	473-437-4027	473-409-3416
Jamaica	Rohan Dawkins	Manager Sales, Cash Management and Merchant Services	876-935-4753	876-832-7572
	Damien Simon	Cash Management Sales Specialist	876-935-4706	876-313-2883
	Wilfred Hermitt	Cash Management Sales Specialist	876-935-4752	876-909-4556
	Calvin Harvey	Cash Management Sales Specialist	876-684-9220	876-322-0168
St. Lucia	Delia Charles-Compton	Cash Management Sales Specialist	758-456-2467	758-484-3171
St. Maarten	Carlos Bignall	Cash Management Sales Specialist	246-467-1942	246-231-0272
St. Vincent	Delia Charles-Compton	Cash Management Sales Specialist	758-456-2467	758-484-3171
Turks & Caicos	Deanna Gardiner	Cash Management Sales Specialist	649-941-1622	649-232-2641

FOR CUSTOMER SERVICE SUPPORT:

FROM TERRITORY	TELEPHONE
Aruba	1-297-582-0018
Antigua, Barbados, BVI, Cayman, Dominica, Grenada, Jamaica, St. Kitts, St. Lucia, St. Vincent, Trinidad & Tobago, Turks & Caicos	1-800-744-1168
St. Maarten	1-844-362-0245
Curaçao	0-800-0247
Nassau, Bahamas	1-242 502-6835
The Bahamas Family Islands	1-242-300-2272

CIBC FirstCaribbean International Bank