Banco de Chile	CLP Not Identifiable Loss | Chilean Peso
USD Not Identifiable Loss | US Dollar	EUR Not Identifiable Loss | Euro
BL0302 - Card Services	EL0102 - Internal Theft & Fraud
CL - Chile	Latin America & Caribbean
Loss Event	Published in media 11 June 2019

Banco de Chile blocks 9,000 cards after employee of ATM provider steals card information

On 11 June 2019, it was reported that Banco de Chile had blocked 8,972 customer cards as a preventative measure after its ATM network provider, Redbanc, suffered a data breach in which the data of 41,594 credit and debit cards was stolen. According to La Tercera, the data was stolen by a former contractor at Redbanc. In total, 13 financial and non-financial institutions were affected, in what La Tercera describes as the largest data breach involving debit and credit cards to have taken place in Chile.

La Tercera reported on 13 June 2019 that Redbanc, a police investigation revealed that the criminal investigation unit of the Santiago de Chile police, OS9 Carabineros had begun investigating a network specialising in cloning bank cards a few months prior. On 1 June 2019, OS9 arrested three suspects and 170 cards were seized.

It was during this investigation that Redbanc was informed on 6 June 2019 that an unauthorised party had stolen the partial information of 41,593 cards used on its network. As of 11 June 2019, 82 cases of fraud had already been recorded, totalling CLP 23 million (approximately USD 33,000), La Tercera reports. Banks will assume liability for the theft of funds.

The alleged perpetrator is a former Redbanc contractor. After stealing card information from Redbanc, the suspect stole a Point of Sale (POS) system from a petrol station on 28 May 2019, and attempted over several days attempted to guess the cards' personal identification numbers (PINs), which he had failed to steal from Redbanc. He did this using new cards he had printed with the information stolen from Redbanc.

On 6 June 2019, OS9 searched the suspect's home, realised that he had worked for Redbanc and subsequently informed the company. Redbanc informed Chile's financial markets commission(CMF) on the same day. On 7 June 2019, the employee failed to arrive at work.

Following the discovery, Redbanc hired a forensic expert to investigate its internal systems, and activated pre-established protocols, which included contacting industry authorities and card issuers. According to La Tercera, Redbanc has relevant insurance. The 13 institutions involved proceeded to preventively block and replace the affected cards and inform the affected customers, Diario Financiero reports.

According to cooperativa.cl, Santander, Scotia Bank, Banco Falabella, Banco BCI and Banco Ripley were also affected by the data breach. While it is not clear how many cards were involved at each institution, Banco Falabella announced on Twitter that it had blocked 6,000 affected cards and Diario Financiero reports that Santander blocked 1,000 cards.

Redbanc said the issue might be the fault of a supplier. On 12 June 2019, Diario Financiero reported that the supplier was the focus of investigations, as it had partial access to the information. However, Chilean Senator Felipe Harboe Bascuñán stated that the data breach occurred because Redbanc did not have adequate security measures regarding its suppliers, cooperativa.cl reports.

As of 11 June 2019, the CMF was continuing to monitor the situation and ensure that all the necessary measures were taken to protect customers. The case was also being investigated by the criminal investigation unit of the Santiago de Chile police, OS9 Carabineros. According to cooperativa.cl, Redbanc has filed a lawsuit against those it claims are responsible, however, the perpetrator has fled the country and, as of 13 June 2019, cannot be found.

Chile's consumer watchdog, SERNAC, has requested information from Redbanc about the cause of the breach, affected institutions, the number of fraudulent transactions detected, mechanisms for reporting the incident, the quantity of complaints it had received, and steps taken to mitigate the effects.

UPDATE

13 June 2019: New details of data breach announced. Headline amended. Paragraphs 1–4 and paragraph 6 amended. Paragraphs 5 and 10 added. Event Type changed from EL0201 External Theft & Fraud to EL0102 Internal Theft & Fraud. Alleged Cause changed from CS0102 Assault by Criminals / Terrorists to CS0203 Criminal Activity by Internal or External Staff. Scenario Category changed from SC0023 Cyber-Related Data Breach to SC0011 Data Breach.

Author: Ashley Whiskerd **Published Date:** 12 June 2019 **Last Update:** 18 June 2019

O.R.X | News

ORX News reference: 8681
ORX Standard: Banking

Published In Media	Occurrence - From	Occurrence - To	Discovery Date	Recognition / Settlement
11 June 2019				

Boundary Risk Other Risk	**Industry Event**	**Scenario** SC0011 - Data Breach
Product PD0401 - Retail Cards	**Process** PC1004 - IT Security	**Event Closed** No
ORX Member No	**Role of Firm** LS0305 - Outsourcer	**Jurisdiction / Choice of Law** LS0103 - Rest of the World
Cause 1 CS0203 - Criminal Activity by Internal or External Staff	**Cause 2**	**Cause 3**
Counterparty LS0207 - Individual - Retail	**Environmental Volatility** LS0406 - Not Identifiable	**Provision** No

Source(s)

https://www.df.cl/noticias/mercados/banca-fintech/cmf-informa-que-se-filtraron-datos-de-mas-41-mil-tarj
http://www.cmfchile.cl/portal/prensa/604/w3-article-26915.html
https://www.cooperativa.cl/noticias/pais/consumidores/los-bancos-afectados-por-el-ciberataque-a-redba
https://www.cooperativa.cl/noticias/pais/consumidores/redbanc-confirmo-filtracion-de-datos-de-41-mil-t
https://www.df.cl/noticias/mercados/banca-fintech/bancos-y-la-mayor-filtracion-de-tarjetas-en-la-historia
https://www.latercera.com/pulso/noticia/tres-detenidos-profugo-la-historia-del-robo-informacion-tarjetas

Related links

https://news.orx.org/node/8384
https://news.orx.org/node/8393