Case 1

NATIONAL CYBERSECURITY ALLIANCE

A Business Trip to South America Goes South

SCENARIO:

A 10-person consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the US, the firm received overdraft notices from their bank. They identified fraudulent withdrawals of $13,000, all originating from South America. There was an additional $1,000 overdraft fee.

ATTACK:

The criminals installed an ATM skimmer device to record card account credentials. Many false debit cards were manufactured and used at ATMs in different cities across South America.

What is Skimming? Skimming occurs when criminals install devices on ATMs, point-of-sale (POS) terminals, fuel pumps, etc. to capture data or record cardholders' PINs. Criminals use the data to create fake debit or credit cards and then steal from victims' accounts.

RESPONSE:

Realizing they had been defrauded, the firm contacted their bank and closed the impacted account immediately. Their attempts to pursue reimbursement from the bank were unsuccessful. The commercial account used at the ATM for local currency had different protections from consumer accounts and the bank was not required to reimburse them for their losses. The bank went on to deduct the $1,000 overdraft fee from the firm owner's personal account.

The firm severed ties with that bank. The new bank offered comprehensive fraud protection guarantees. The firm created two business accounts:

- one for receiving funds and making small transfers
- one for small expense payments

The firm updated travel protocols, banning the use of company-provided debit cards. Employees now prepay expenses electronically, pay cash, or use a major credit card, as necessary.

IMPACT:

The entire cash reserve for the small business was wiped out, netting losses of almost $15,000.

LESSONS LEARNED:

1. Use major credit cards when traveling - they have more consumer fraud protection than debit cards.
2. Get notified - set up transaction alerts with your credit and debit card companies to monitor fraud.
3. Check your bank account frequently.
4. Create withdrawal alerts.
5. Understand your bank's policies about covering losses from fraud.

DISCUSS:

- Knowing how the firm responded, what would you have done differently?
- What are some steps you think the firm could have taken to prevent this incident?
- Is your business susceptible? How are you going to reduce your risk?

RESOURCES:

- NIST Small Business Cybersecurity Corner: https://www.nist.gov/itl/smallbusinesscyber
- National Cybersecurity Alliance: https://staysafeonline.org/cybersecure-business/

This resource, funded through NIST Federal Award 70NANB19H165, is intended to be used for general education purposes. The content of the case studies is a combination of publicly available information, business-submitted information, and fictional details to create an educational scenario.