ATM Skimming Communications Playbook

Overall Crisis Communications Objectives

- Provide support for your members
- Protect your credit union brand
- Guide credit union employees in best practices
- Seek to minimize misunderstanding and misinformation
- Create a sense of stability and counter anxiety
- Establish transparency
- Manage news coverage
- Manage social media activity

Crisis Communications Best Practices for ATM Skimming Incidents

- Identify your credit union's crisis communications team – including spokesperson(s) and social media manager(s) – and establish roles to be best prepared ahead of an event
- Set up monitoring on social media and media platforms in order to stay abreast of conversations and coverage
- Develop messaging for your members and a media statement to be used for media inquiries. When developing statements and messaging, consider the following to establish the facts:
  - During what time frame did the skimming incident(s) occur?
  - Where did the incident(s) occur?
  - Who has been affected by the incident(s)?
  - What steps are being taken to resolve the incident(s)?
  - How long until operations return to normal?
  - Have there been any member inquiries?
  - Have there been any media inquiries? If so, from who?

Overview

While the vast majority of ATM and gas pump transactions are conducted safely and securely, fraud can and does happen. ATM skimming is a type of fraud that occurs when a terminal has been compromised by a skimming device (or "skimmer"), which contains a card reader that can be disguised to look like part of the card terminal. Fraudsters place these skimmers on or in a card reader, collecting card numbers and PIN codes which can then be replicated into counterfeit cards.

This document is intended to provide credit unions with communications guidelines and assistance during ATM skimming incidents, which can impact a credit union and its members with no notice. The below guidelines can help your credit union prepare for this crisis and respond appropriately.

Dissemination of Information

- Ensure all member-facing staff are aligned on approved messaging that should be used with members
- Any information relayed to the media should be communicated through a designated spokesperson(s); all staff should be advised not to speak with the media and that any inquiries should be directed to the designated spokesperson(s)
- Any information shared via social media should be communicated though a designated social media manager(s)
- Key stakeholder groups are as follows:
  - **Internal**
    - Credit union employees
    - Credit union board
  - **External**
    - Credit union members
    - Media

Proactive vs. Reactive Response

In some situations, it is in your best interest to only reactively respond to inquiries from certain stakeholders as opposed to proactively distributing information:

- Proactively share information with members via your credit union's website, contact center and through other educational materials in order to help them be better prepared to spot a skimmer and prevent incidents
- Proactively communicate with members via the aforementioned channels if an ATM skimming incident occurs at your ATMs or in your local area at gas stations, etc. that has been confirmed to impact members
- Proactively provide employees with information about ATM skimming, particularly member-facing employees, in order to answer member questions as necessary and assist with education to prevent incidents
- Proactively alert employees if an ATM skimming incident occurs, particularly member-facing employees as they may receive inquiries from members on the issue
- Reactively respond to media as inquiries are received

Sample Media Statement

Your team should have a media statement prepared in case of an incident. Below is a sample media statement that can be updated as necessary to fit your particular situation(s):

On [date], [credit union name] confirmed that our [ATM(s); gas stations in our area; etc.] had skimming device(s) fraudulently installed on [our; its] machine(s). We are in the process of working directly with members impacted by this incident and taking additional steps to block possible fraud and ensure safety at all of our ATMs. We are also working in conjunction with local authorities to combat future incidents.

For assistance, further questions, if you suspect ATM skimming or if you've been the victim of ATM skimming, contact us right away. Please [visit our website, visit your nearest branch or call us at XXX-XXX-XXXX, etc.].

Media Guidelines

When interacting with the media, only your designated spokesperson(s) should speak with reporters and/or media outlets. Your credit union's designated spokesperson(s) should follow these guidelines when speaking with media and/or providing statements following an ATM skimming incident:

- Only provide factual information; never speculate
- Never answer a question with "no comment"; always give the reason why he/she cannot answer the question at that time – if he/she does not know the answer, offer to find out
- Speak calmly and deliberately in order to convey that your credit union is in control of the situation
- Never speak with media "off the record"
- Always have a prepared statement to help ensure that you disclose the same information to all media

- Keep detailed notes of the information that is disclosed; advise media immediately when/if important information is reported inaccurately
- Keep statements simple—focusing on who, what, when, where, why, and how—and avoid jargon
- Be authentic; never use sarcasm or humor in crisis situations
- Emphasize good news (if any) and reinforce your credit union's key brand messaging at appropriate opportunities
- Never violate the privacy of staff

Member-Facing Employee Guidelines

Your credit union's member-facing employees (those who may receive calls or inquiries at branch locations) should follow these guidelines during an ATM skimming situation:

- Once an official statement has been approved, respond to questions using this information only
  - Responses should mirror information provided by the spokesperson(s)
- If additional information is available via another source (your credit union's online newsroom, for example), information on how to access this should be provided when it becomes available (i.e. how to avoid ATM skimming, etc.)
- Only provide factual and pre-approved information; never speculate
- Keep detailed notes of the information disclosed

Social Media Guidelines

Your credit union's designated social media manager(s) should follow these guidelines during a crisis situation:

- Once an official statement has been approved by your team, post a pre-approved message on all social media platforms for proactive situations
  - This message should mirror information provided by the spokesperson(s)
- If additional information is available via another source (your credit union's online newsroom, for example), a link should be provided when it becomes available
- Continue to monitor conversation in real-time on an ongoing basis; respond with pre-approved general messages(s) reactively as necessary

Sample Social Media Statement

The statement below can be modified for your credit union's certain social media platforms. For example, the statement in its entirety can be posted on Facebook but might need to be shortened to meet Twitter's character limit. Do not post information on Instagram, as you cannot include links to further information in posts via this platform.

On [date], [credit union name] confirmed that our [ATM(s); gas stations in our area; etc.] had skimming device(s) fraudulently installed on [our; its] machine(s). We are in the process of working directly with members impacted by this incident and taking additional steps to block possible fraud and ensure safety at all of our ATMs. For assistance, further questions, if you suspect ATM skimming or if you've been the victim of ATM skimming, contact us right away. Please [visit our website, call us at XXX-XXX-XXXX, etc.].

Sample Website Content to Utilize After an ATM Skimming Incident

Below is a sample statement to be posted on your website that can be updated as necessary to fit your particular situation(s):

On [date], [credit union name] confirmed that our [ATM(s); gas stations in our area; etc.] had skimming device(s) fraudulently installed on [our; its] machine(s). We are in the process of working directly with members impacted by this incident and taking additional steps to block possible fraud and ensure safety at all of our ATMs. We are also working in conjunction with local authorities to combat future incidents.

For assistance, further questions, if you suspect ATM skimming or if you've been the victim of ATM skimming, contact us right away. Please [visit our

website, visit your nearest branch or call us at XXX-XXX-XXXX, etc.].

For more information on how to protect yourself, visit the resources below:

- What is ATM Skimming
- How to Spot ATM Skimming
- How to Prevent ATM Skimming

Recommended Information to Share with Members on an Ongoing Basis

PSCU recommends sharing the below information with your members in order to educate them on how to spot skimmers and prevent incidents. This information should be posted on your website, available to all member-facing employees and in branches as pamphlets. On social media, share links to these resources on an ongoing basis as well in order to boost member education.

What is ATM Skimming

ATM skimming is a type of fraud that occurs when a terminal has been compromised by a skimming device or skimmer. A skimmer is a device that contains a card reader that can be disguised to look like part of the card terminal. Fraudsters place a small device "skimmer" on or in a card reader that collects card numbers and PIN codes, which are then replicated into counterfeit cards.

ATM skimming fraud is on the rise, and we want our members to be aware what to look for at ATMs, gas pumps, and anywhere a debit or credit card is used.

How to Spot ATM Skimming

Help protect your financial information by being on the lookout for the following:

- **Skimming Overlay Devices:** These devices are placed over a card slot. When a card is inserted into the slot, the device records the card's magnetic stripe data.
- **Deep Insert/Shimming Technology:** Thieves install a thin, card-size device with a microchip into the card slot. This device, which isn't visible from the outside of the ATM or gas pump, steals information that allows the thief to clone your card. Sometimes fraudsters must file the card slot to insert these, so there may be debris or the card slot may appear altered.
- **Keypad Overlays:** These devices are placed over a keypad and can capture PINs as they're entered.
- **Tiny Cameras:** Cameras can be used in conjunction with skimming devices. The camera is placed in a location on the ATM or gas pump in order to record the user entering his or her PIN. Many skimming devices transmit information back to fraudsters using Bluetooth technology. However, some crooks could also be watching you enter your PIN with binoculars or by looking over your shoulder.

How to Prevent ATM Skimming

- **Scrutinize the ATM:** Look for signs that the ATM might have been altered – parts that look crooked, a loose card reader, loose or spongy ATM keys, etc. If there is another ATM nearby, compare the two to see if there are obvious differences.
- **Be choosy:** Visit high-traffic and high profile ATMs and gas pumps. Avoid gas pumps that are out of sight of the clerk and ATMs in areas with little traffic.
- **Cover the PIN pad:** This prevents cameras and nearby thieves from seeing your PIN.
- **Pay inside:** There is less chance a fraudster placed a card skimmer on the payment terminal in front of the clerk inside the gas station or convenience store.
- **Be vigilant:** Be observant of your surroundings. Stand directly in front of the ATM while using it and watch for anyone standing too close. Also, check your accounts regularly and set up fraud alerts to be notified of any potential fraud right away.

If you suspect ATM skimming at one of our ATMs or if you've been the victim of ATM skimming, contact us right away. Please [visit our website, visit your nearest branch or call us at XXX-XXX-XXXX, etc.].