Office of Banking Notice of Cybersecurity Event

All State Chartered Banks must notify the Director promptly after determining a cybersecurity event occurred involving nonpublic information in the institution's possession. An authorized representative from the institution should complete this form or provide a documented notice that includes the pertinent information contained herein. Pursuant to the reporting requirements of section 487.13911 of the Michigan Banking Code, institutions are required to notify the commissioner as to the condition of the bank, which includes cybersecurity events.

It is requested that institutions update and supplement this form regarding material changes to information previously provided relating to the cybersecurity event. Please provide as much information as possible in completing this form.

Note: This form and attachments should be submitted as a single PDF document and sent to email address: MI-DIFS-Banking@michigan.gov

---

☐ Initial Report of Cybersecurity Event	☐ Subsequent Report Updating or Supplementing Initial Report of Cybersecurity Event

Section 1 – Information of Financial Institution

Institution Name		Charter Number
Submitter's First Name	Submitter's Middle Name	Submitter's Last Name
Institution Address		
Suite/Apartment/Building		
City	State	Zip Code
Telephone		Fax
Email Address		

Section 2 – Cybersecurity Event Dates

Estimated Occurrence:	Estimated End:	Date Discovered:

Section 3 – Event Type (Check all that apply)

☐ Data theft by employee/contractor
☐ Hacker or unauthorized access
☐ Lost
☐ DDOS Attack
☐ Phishing
☐ Improperly released, exposed, displayed
☐ Stolen laptop(s)
☐ Other
☐ Computer and equipment
☐ Improperly disposed
☐ Ransomware Attack

Other:

Section 4 – Circumstances Surrounding the Cybersecurity Event

Did the cybersecurity event occur within the information or systems maintained by the institution or within the information or systems maintained by a third-party service provider? (Check the applicable box.)

☐ Institution's information or systems

☐ Third-party service provider's information or systems

Name:

Description:

Specific Roles and Responsibilities:

How was the information exposed, lost, stolen, or breached?

How was the cybersecurity event discovered?

What is the identity of the source of the cybersecurity event?

Section 5 – Specific Type(s) of Information

Check the specific type(s) of information that were acquired without authorization.

Identifying Information:	Financial Information:
☐ Name	☐ Commercial Deposit or Loan Information
☐ Date of Birth	☐ Consumer Deposit or Loan Information
☐ Address	☐ Credit or Debit Card
☐ Mother's Maiden Name	☐ Other:
☐ Driver's License	
☐ Social Security Number	
☐ Passport	
☐ Other:	

If the specific type(s) of information acquired without authorization is not listed above, provide a description.

Was the electronic information involved in the cybersecurity event protected in some manner?

☐ Yes	☐ No	☐ Only non-electronic information was involved

Section 6 – Number of Consumers in Michigan Affected by Cybersecurity Event

Provide the total number of Michigan residents affected by the cybersecurity event whose nonpublic information is in the institution's possession, custody, or control.

Best Estimate:

Section 7 – Law Enforcement

Has a police report been filed? If so, provide the date of the report. (Note: A copy of the report is requested.)

☐ Yes Date of Report: Name of Police Agency:	☐ No

Has a regulatory, government, or law enforcement agency been notified? If so, provide the date of the notice.

☐ Yes Date of Report: Name of Agency:	☐ No

Section 8 – Institution Response

Has any lost, stolen, or breached information been recovered, and if so, how was the information recovered?

If an Internal Review identified a lapse in either automated controls or internal procedures or confirmed that all automated controls and internal procedures were followed, provide a description of the results.

☐ Identified lapse in automated controls or internal procedures Results:	☐ Confirmed automated controls and internal procedures were followed Results:	☐ No Internal Review has yet been completed

Describe the efforts undertaken to remediate the situation that permitted the cybersecurity event to occur.

Provide a statement outlining the steps that will be taken to investigate and notify consumers of the cybersecurity event.

Is notice to impacted Michigan residents and/or entities required under state or federal law?

☐ Yes Date of notice if provided: (Note: Copy of notice sent or draft will be required below.) Intended date of future notice if not yet provided:	☐ No	☐ Unknown at this time

Section 9 – Contact Information of Individual Familiar with the Cybersecurity Event and Authorized to Act on Behalf of Institution

☐ The authorized individual is identified in Section 1 and his or her contact information is the same as provided in Section 1.

☐ The authorized individual is not identified in Section 1 or his or her contact information is different than as provided in Section 1. If this box is checked, provide the below contact information.

First Name	Middle Name	Last Name
Address		
Suite/Apartment/Building		
City	State	Zip Code
Telephone	Fax	
Email Address		

Section 10 – Submission and Attachments

This form and attachments should be submitted as a single PDF document and sent to email address: MI-DIFS-Banking@michigan.gov

Mandatory attachments:

1. A copy of the institution's Incident Response Plan.
2. A copy of any notice or notices sent to consumers.
3. Any documents that are necessary to adequately respond to the questions in this form.

Institutions are encouraged to provide any additional information or documentation that may be relevant to the cybersecurity event, including, but not limited to, the following:

1. A copy of a police report or notice sent to a regulatory, government, or law enforcement agency.
2. A copy of an Internal Review Report that either identified a lapse in automated controls or internal procedures or confirmed that all automated controls and internal procedures were followed.
3. Any additional relevant correspondence or information.

Section 11 – Attestation

I attest to the best of my knowledge that the information submitted on or attached to this form is true, correct, and completed to the best of my information and belief. By submitting this form, I am acknowledging that I am authorized to submit this form on behalf of the Institution.

Signature of institution's authorized representative

Date signed

Authorized representative's name and title (print or type)