"Huge mess of theft and fraud:' artists sound alarm as NFT crime proliferates"[5]

Art Guardian

Team Blue

CS411 Fall 2022 Prototype Presentation

Table Of Contents

Planned Approach

- Agile Sprints:
  - 5 Sprints in Total
  - Sprints will last three weeks
- Scrums:
  - Three scrums per sprint
  - One scrum per week
  - Two hours
  - Report on Individual Progress
  - Conducted on Discord
- Sprint Task Planning:
  - Tasks will be selected by team members.
  - Team will split into groups based on selection.

Team Blue

Carlo Diaz
Frontend/Webmaster

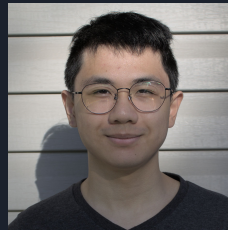Paolo Ihde
Frontend/Backend

Brandon Kidd
Database Specialist/Backend

Michael Thompson
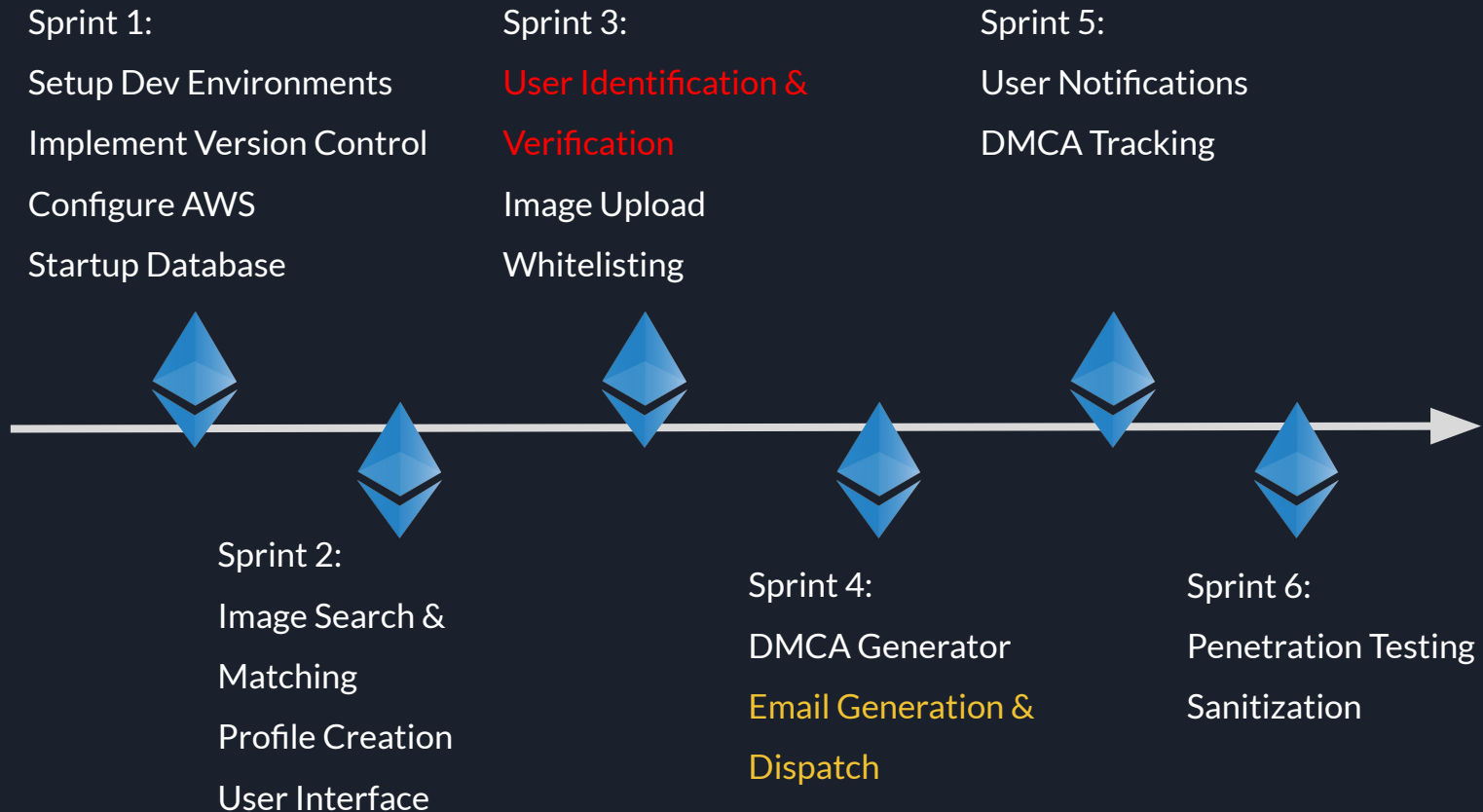Backend/Frontend

Autumn Roberts
Team Leader/Frontend

Tobin Zheng
Backend / Web Master

Spencer Hite
Database Specialist/Backend

Development Plan: Agile Sprints

Sprint 1:

Setup Dev Environments

Implement Version Control

Configure AWS

Startup Database

Sprint 3:

User Identification & Verification

Image Upload

Whitelisting

Sprint 5:

User Notifications

DMCA Tracking

Sprint 2:

Image Search & Matching

Profile Creation

User Interface

Sprint 4:

DMCA Generator

Email Generation & Dispatch

Sprint 6:

Penetration Testing

Sanitization

Timeline

Sprints		OCT	NOV	DEC	JAN '23
	Sprint 1	Sprint 2	Sprint 3	Sprint 4	Sprint 5, Sprint 6	
BL411-33 Setup dev environments	████					
BL411-34 Setup cloud services and database	████					
BL411-35 Create fake NFTs for testing purposes		████				
BL411-36 NFT detection backend work		████				
BL411-37 Implement image matching		████				
BL411-38 Implement account creation			████			
BL411-39 Implement art upload and gallery			████			
BL411-40 Implement DMCA takedown				████		
BL411-41 Setup user notifications and DMCA tracking					████	
BL411-42 Create static pages for app tutorial/guidelines					████	
BL411-43 Implement testing					████	

Development Tools

Platform		
Component		Desktop Web App
	Language	HTML, CSS, Javascript, Python
	Frameworks	React
	IDE	Visual Studio Code
	Database	Amazon RDS And Amazon S3
	Version Control	Git
	Issue Tracking	GitHub
	Documentation	jsdoc
	Services	AWS Amplify

RWP vs Prototype

Fully Implemented

Partially Implementing

Eliminated

Art Guardian	RWP	CS411W Prototype
Account Creation	Fully Implemented	Fully Implemented
User Verification	Fully Implemented	Eliminated: Mock data
Art Upload	Fully Implemented	Fully Implemented
Art Tutorial	Fully Implemented	Fully Implemented
Image Library	Fully Implemented	Fully Implemented
Whitelisting	Fully Implemented	Fully Implemented
Marketplace Monitoring	Fully Implemented	Fully Implemented
Image Matching	Fully Implemented	Fully Implemented
Stolen Art Alert	Fully Implemented	Fully Implemented
DMCA Generation	Fully Implemented	Fully Implemented
DMCA Filing	Fully Implemented	Partially Implemented: Send to testing email
DMCA Cataloging	Fully Implemented	Fully Implemented
DMCA Tracking	Fully Implemented	Eliminated: Simulated Data

User Stories

Fully Implemented   Partially Implementing   Eliminated

Artist:

As an artist, I need to be able to sign in to my account to access the app.

As an artist, I need to be able to sign up for an account to join and protect my art.

As an artist, I need to be able to reset my password in case I forget my password.

As an artist, I would like a tutorial on how to use the app so I can properly protect my art.

As an artist, I need to be able to upload my art to keep my art safe.

As an artist, I would like to see a collection of the art that I have uploaded in order to know what is or is not protected.

As an artist, I would like to know which pieces of my art have been found on the NFT marketplaces so I can take further action.

As an artist, I would like to see information to help me protect my art so I can prevent theft.

As an artist, I would like to be able to issue takedowns of stolen art found on the marketplace so I can prevent an illegal sale.

As an artist, I would like Art Guardian to automatically generate DMCA takedowns for stolen art so I do not have to do that myself.

As an artist, I would like to be updated on the status of the DMCA Takedown so I can know when it is taken down or if I have to take further action.

As an artist, I need my information to be secure and private so I can remain anonymous.

As an artist, I would like to see information about the NFT using my art so I can see who stole it and what marketplace it is on.

As a NFT Artist I need to be able to whitelist my minted NFT so my own NFT doesn't trigger a theft alert.

Tester User Stories

Fully Implemented   Partially Implementing   Eliminated

Tester
As a tester I need to be able to trigger the 2-Factor-Authentication for testing.
As a tester I need to be able to trigger a push notification for testing.
As a tester I need to be able to access the image database for reading and uploading images.
As a tester I need to be able to make a fake NFT to test our DMCA Generation system.
As a tester I need to be able to make a fake NFT to test our flagging system.
As a tester I need to be able to invoke the image matcher to receive test matching values.
As a tester I need to be able to make a fake NFT to test our Whitelisting system.
As a tester I need a testing mode for our app to access tests easier.
As a tester I need to be able to access the image database for reading and writing user information.
As a tester I need to be able to verify my identity using the Stripe-API.
As a tester I need to be able to access the email API to send test emails.

User Stories To Features

Feature	User Story
Account Creation	• As an artist, I need to be able to sign in to my account to access the app • As an artist, I need to be able to sign up for an account to join and protect my art. • As an artist, I need to be able to reset my password in case I forget my password.
Art Scanning	• As an artist, I would like to know which pieces of my art have been found on the NFT marketplaces so I can take further action.
App Tutorial	• As an artist, I would like a tutorial on how to use the app so I can properly protect my art. • As an artist, I would like to see information to help me protect my art so I can prevent theft.
Art Upload	• As an artist, I would like to see a collection of the art that I have uploaded in order to know what is or is not protected.
DMCA Catalogue	• As an artist, I would like to be updated on the status of the DMCA Takedown so I can know when it is taken down or if I have to take further action.
DMCA Generator	• As an artist, I would like Art Guardian to automatically generate DMCA takedowns for stolen art so I do not have to do that myself.

User Stories To Features

Feature	User Story
Issue DMCA Takedowns	● As an artist, I would like to be able to issue takedowns of stolen art found on the marketplace so I can prevent an illegal sale.
Two-Factor Authentication	● As an artist, I need my login information to be secure with 2-Factor-Authentication.
Push Notifications	● As an artist I want to be notified when stolen are is found so I can take immediate action.
Whitelisting	● As a NFT Artist I need to be able to whitelist my minted NFT so my own NFT doesn't trigger a theft alert.

Desktop Web App UI/UX: Sign Up and Login

ART
GUARDIAN

USERNAME

PASSWORD

LOGIN

SIGNUP

SIGN UP

EMAIL

USERNAME

PASSWORD

RE-TYPE PASSWORD

FIRST NAME

LAST NAME

PHONE NUMBER

SUBMIT

Link an Art Account

?

Verify Identity
with ID scan

Desktop Web App UI: Home and Art Library

ART GUARDIAN

Welcome back, John Doe

Today, we found 1 instance of theft

Click here, or check your notifications for more info

Art Protection Guidelines

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc lacinia ut ligula a facilisis. Phasellus et lacus eget magna blandit molestie
- non et ex. Donec quis dignissim nunc. Nam commodo ex quis auctor
- sollicitudin. Morbi eu fringilla eros. Maecenas eu leo auctor,
- interdum nisl fringilla, maximus tortor. Nam in libero a dolor lacinia eleifend ac non dui.
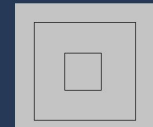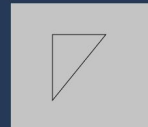
ART GUARDIAN

John Doe

6 art pieces

Upload art

Art Library

Desktop Web App UI: Art Upload and Notifications

ART GUARDIAN

Upload your art

*Required

Title
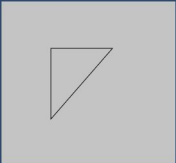
Add File
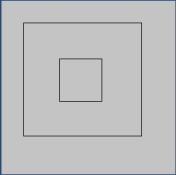+

Files must be in .foo, .bar, or .baz format

Upload

ART GUARDIAN

Your art titled "Triangle" has been found on an OpenSea transaction

Click here for more information
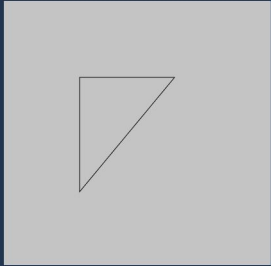
Your art titled "Squares" has been found on an OpenSea transaction

Click here for more information

Desktop Web App UI: DMCA Takedown

ART GUARDIAN

IMPORTANT, PLEASE READ
By continuing further, confirm that:

You ARE the ORIGINAL artist of this piece of artwork

☑ *Required

You ARE looking to request a takedown of this NFT

☐ *Required

Marketplace: OpenSea
URL: opensea.io/..............
Blockchain: Ethereum
Token: 0x000000000000000
User: Jane Doe

CONTINUE

*Both boxes must be checked off before continuing

ART GUARDIAN

DMCA Takedown Request

To OpenSea,
Art Guardian is acting on behalf of the copyright owner of the art "Triangle".
[link and token ID would go here]
This letter is official notification under the provisions of Section 512(c) of the Digital Millennium Copyright Act ("DMCA") for removal of the above-referenced copyright infringement(s). Art Guardian hereby requests that you immediately issue a cancellation message as specified in RFC 1036 for the specified postings and prevent the infringer, who is identified by its Web address, from posting the infringing art to your servers in the future. The law requires you to "expeditiously remove or disable access to" the infringing works of art upon receiving this notice. As a service provider, noncompliance may result in a loss of immunity for liability under the DMCA as cited above.

I have a good faith belief that use of the material in the manner complained of herein is not authorized by the copyright holder, or the law. The information provided is true and accurate to the best of my knowledge. I swear under penalty of perjury that I am the copyright owner or have the authority to act on behalf of the copyright owner.
Sincerely,
Art Guardian
Email
Address
Phone Number

Required

X_____

SUBMIT E-SIGNATURE

Issues / Challenges

- Steep learning curve
  - Divide and Conquer
- Scope bounding
  - Limit NFT marketplaces
  - Limit search frequency
- Time constraints
  - Task delegation
  - Large workloads
- Sources of mock data
  - User accounts
  - Test art
  - Test NFTs
  - Test DMCA
  - Test email

Technical Risk Matrix

CS411W Prototype

Impact						
		Very Low	Low	Medium	High	Very High
Probability	Very High	🟨	🟨	🟥	🟥	🟥
	High	🟨	🟨	🟨	🟥	🟥
	Medium	🟩 T-1 T-2	🟨 T-2	🟨 T-1	🟨	🟥
	Low	🟩	🟩	🟨	🟨	🟨
	Very Low	🟩	🟩 T-4	🟩	🟨 T-4	🟨 T-3

Blue - Post Mitigations

Technical Risks

- T-1: Matching API yields a false match.
- T-2: Market does not comply with DMCA.
- T-3: ID API does not correctly verify identity.
- T-4: Automatic DMCA has wrong information

Technical Risk Mitigations:

- T-1: User verifies art is theirs before sending DMCA.
- T-2: Flag art that reappears in the market place and notify user.
- T-3: Multiple ways to submit ID information.
- T-4: Final verification check.

Customer Risk Matrix

	Impact					
		Very Low	Low	Medium	High	Very High
Probability	Very High	🟨	🟨	🟥	🟥	🟥
	High	🟨	🟨	🟨	🟥	🟥
	Medium	🟩	C-2	🟨	C-1	🟥
	Low	🟩	C-2	🟨	🟨	🟨
	Very Low	🟩	C-3	C-3	C-1	🟨

Blue - Post Mitigations

Customer Risks

- C-1: Users abuse the system by uploading/issuing DMCA for art they do not own.

- C-2: User doesn't know how to use the app.
- C-3: User forgets to issue the DMCA.

Customer Risk Mitigation

- C-1: Sign up using art accounts.

- C-2: Integrated User Tutorial.

- C-3: Timer that reminds user to cancel or send the DMCA

Security Risk Matrix

CS411W Prototype

Impact						
		Very Low	Low	Medium	High	Very High
Probability	Very High	🟨	🟨	🟥	🟥	🟥
	High	🟨	🟨	🟨	🟥	🟥
	Medium	🟩	🟨	🟨	🟨	🟥
	Low	🟩	🟩	S-1	🟨	S-2
	Very Low	🟩	🟩	S-1	S-2	🟨

Blue - Post Mitigations

Security Risks

- S-1: Unauthorized access to a user account.

- S-2: Database Integrity.

Security Risk Mitigation:

- S-1: Two Factor Authentication for Login.

- S-2: Use Secure Databases and Encrypt user data (AWS)

Thank You for Participating!
Any Questions?