SCAMMED!- A cautionary tale and a defense strategy
Today’s Topics

• About UC San Francisco
• How the Scam was Executed
• The Response: Immediate Stop Gaps and Long Term Key Controls
• PaymentWorks Supplier Onboarding System
• FICO Risk Assessment
About UC San Francisco

- A graduate university with 4 schools in medicine, dentistry, nursing and pharmacy with 3,300 students, 1,500 clinical residents and 1,000 postdoctoral scholars
- In 2017, for the sixth year in a row, the UCSF School of Medicine is the top recipient of NIH funding among all medical schools in the country
- Received $593.9 million funding in 2017
- UCSF Medical Center has been named among the nation’s premier medical institutions for the 17th consecutive year, ranking as the fifth best hospital in the country and the top-ranked hospital in California, in U.S. News & World Report’s 2017-2018 Best Hospitals survey
**ACH Enrollment Form**

**Electronic Funds Transfer Authorization**

- **New Request** (Not available to individuals)
- **Account Change**
- **Cancel**

### PAYEE/COMPANY INFORMATION

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td></td>
</tr>
<tr>
<td>ADDRESS</td>
<td></td>
</tr>
<tr>
<td>CITY, STATE, and ZIP+4 CODE</td>
<td>OAKLAND, CA, 94612-3520</td>
</tr>
<tr>
<td>A/R CONTACT NAME</td>
<td>RAUL ROSALES</td>
</tr>
<tr>
<td>A/R CONTACT PHONE</td>
<td>510-400-5971</td>
</tr>
<tr>
<td>BUSINESS EMAIL ADDRESS</td>
<td><a href="mailto:RAUL.ROSALES@KANSAK-BUILDING.COM">RAUL.ROSALES@KANSAK-BUILDING.COM</a></td>
</tr>
<tr>
<td>EMPLOYER ID NO (EIN)</td>
<td></td>
</tr>
<tr>
<td>DUNS NUMBER</td>
<td></td>
</tr>
</tbody>
</table>

### FINANCIAL INSTITUTION INFORMATION (MUST BE A BUSINESS ACCOUNT)

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPOSITORY INSTITUTION NAME</td>
<td></td>
</tr>
<tr>
<td>ADDRESS</td>
<td>11222 S. SAM HOUSTON PKWY EAST</td>
</tr>
<tr>
<td>CITY, STATE, and ZIP+4 CODE</td>
<td>HOUSTON, TX, 77089</td>
</tr>
<tr>
<td>TRANSIT ROUTING NUMBER</td>
<td></td>
</tr>
<tr>
<td>ACCOUNT NUMBER</td>
<td></td>
</tr>
<tr>
<td>ACCOUNT TYPE</td>
<td></td>
</tr>
<tr>
<td>ACH FORMA</td>
<td></td>
</tr>
<tr>
<td>DTS</td>
<td></td>
</tr>
</tbody>
</table>

### FOR CTX ONLY

- Please note the option for electronic payment using CTX format requires initial testing to validate the service is critical to provide the information below. The EDI Implementation Guide will be sent to the IT/EDI contact.

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT/EDI CONTACT NAME</td>
<td></td>
</tr>
<tr>
<td>IT/EDI CONTACT EMAIL</td>
<td></td>
</tr>
<tr>
<td>IT/EDI CONTACT PHONE</td>
<td></td>
</tr>
</tbody>
</table>

**IMPORTANT NOTE:** The person signing the Authorization must be a designated officer from the Finance Department and a person other than the contact listed above.

### AUTHORIZATION

I hereby authorize the University of California San Francisco (UCSF) to initiate electronic transfer of funds to the account stated above using the National Automated Clearing House (NACHA) Cash Concentration or Disbursement (CCD) or Corporate Trade Exchange (CTX) for settlement of invoices. If funds to which I, or the company I represent, am not entitled are deposited in the account stated above, I authorize the University to initiate a correcting (debit) entry. This authorization will remain in effect until UCSF receives written notification of its termination. I understand payment details will be sent to the business email address provided above (applies to CCD only).

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNATURE</td>
<td></td>
</tr>
<tr>
<td>DATE</td>
<td>07/24/2017</td>
</tr>
</tbody>
</table>

**PRINT NAME**

**TITLE**

CHIEF FINANCIAL OFFICER

***PLEASE ATTACH A VOIDED CHECK TO CONFIRM ACCOUNT INFORMATION***

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMAIL (preferred):</td>
<td><a href="mailto:verdres@ucsf.edu">verdres@ucsf.edu</a></td>
</tr>
<tr>
<td>MAIL:</td>
<td>UCSF Supply Chain Management</td>
</tr>
<tr>
<td>C/O:</td>
<td>Supplier Registration</td>
</tr>
<tr>
<td>ADDRESS:</td>
<td>1855 Folsom St Ste 304</td>
</tr>
<tr>
<td>CITY:</td>
<td>San Francisco, CA 94110</td>
</tr>
<tr>
<td>ZIP+4 CODE:</td>
<td>94110</td>
</tr>
</tbody>
</table>

Version 17.1
How the Scam Occurred

- Fraudster sent request to UCSF to update ACH electronic payment banking information
- Processed request as routine operating procedure
- Payment intended for a construction contractor issued to the fraudster’s account
The Response

- Implemented immediate stop-gaps which prevented a second identical fraud the next day
- Police report and Risk Management insurance report
- Task force formed with senior leadership sponsorship
- Determine additional exposure
- Implement key controls to prevent recurrence of this type of fraud
- Risk mitigation solutions using sophisticated front-end and back-end systems
Fraud Attempt of $4M Caught

Watch Items:
- Email format
- Suspicious address
- Poor grammar or words (foreign use)

Key Controls:
- Obtain positive confirmation from supplier on changes
- Compare old bank information on request form against existing record on file

From: Skanska USA Building Inc. <accounts@skanska-usa.com>
Sent: Monday, January 22, 2018 9:25 AM
To: Supply Chain Management - Vendors
Subject: Suppliers id: 00302354 Account update

Good Afternoon sir,
Following our conversation earlier we are notifying you that we have recently updated our payment system form cheques payments to electronic payment and we want you to change our payment method the last cheques we received is (Cheque No. 2985743 – $4007217.05 dated—12/21/2017, this cheque has not yet been cashed)
If agreed we will send you our account details for you to update so we can receive all invoice payments asap.

Kind Regards
Oliver Daniels
Accounts Department

[Address and other details removed]

MAILSERVER NOTICE: This message contains confidential information and is intended only for the individual named. Skanska USA Building Inc. accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information provided. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Skanska USA Building Inc. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. If you have received this email in error please notify the system manager or the sender immediately and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message or any damage caused by any virus, which arise as a result of e-mail transmission. The recipient should check this email and any attachments for the presence of viruses.
Fraud Attempt of $4M Caught

<table>
<thead>
<tr>
<th>Payee/Company Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: C.D. Avila Pena (paymaster on behalf of)</td>
</tr>
<tr>
<td>Address: 1999 Harrison Street, Suite 1500 Oakland, California 94612</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A/B Contact Name</th>
<th>A/B Contact Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oliver Daniels</td>
<td>+1 510 285 1810</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Account Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Number:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Previous Banking Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Payments: Check No: 2985743</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New Banking Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>citibank NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maintenance Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA Routing Number:</td>
</tr>
<tr>
<td>Bank Account Number:</td>
</tr>
<tr>
<td>Type of Account: Checking</td>
</tr>
</tbody>
</table>

We hear by confirm that the above information is true and correct.

Sincerely,

Rudolf Ludwig
Account Manager

---

**NOTICE:** This document is marked as **SCAM**.
Front-end System - PaymentWorks

PaymentWorks is an ERP agnostic, cloud-based supplier portal solution that automates all (or most of) the communications between companies and their suppliers around onboarding and information update:

- Automate new vendor registration process through supplier portal
- Configurable business rules /controls/approval workflow
- ITS Tax Identification Number (TIN) check, debarred suppliers check
- Data integration with ERP
Falcon Assurance Navigator (FAN)
Next Gen in Fraud, Waste, and Abuse across procure to pay cycle

High-level Features

- Monitor 100% of transactions in-line, real-time, across all phases across the procure to pay cycle
- Apply different risk criteria for different state funds – enhanced financial management
- Employ a two-pronged approach: expert rules and advanced anomaly detection algorithms
- Review prioritize transactions based on data-driven risk assessments

Transaction Types

- T&E Reimbursement
- P-Cards
- Invoices (Ext./Int billing)
- Procurement (Req & PO)

Transaction Types

- T&E Reimbursement
- P-Cards
- Invoices (Ext./Int billing)
- Procurement (Req & PO)
Risk-based Framework Components – High Risk Areas & Value Proposition

- Compliance Risks (e.g. HIPAA, Data security/Privacy, PCI)
- PO Leakage and Excessive Spend
- Funding sources – Unallowable Costs
- Excessive Travel & Non-business related Reimbursement

Review rates/Costs

Risk Mitigation/Cost Savings
In-line Vendor Monitoring (block payment)

Invoice Transaction Processing Workflow

Validation → Accounted → Payment

Potential “trigger” points

FAN

Bank Account Changes
Vendor TIN/Employee SSN Matches
Vendor/Employee Address Matches

FAN Vendor Strategies:

Managed Service

Rules

Analytics
FAN – Risk Reduction & Cost Savings Use Cases

**Risk Reduction**
- HIPAA
- IT/Cloud
- Open Source/IP

**Cost Savings**
- T&E (P-card/PO)
- P-card (PO, Excessive)
- Suppliers (Strategic – Consolidation)
- Invoices (Non-PO, After the Fact, Duplicates, Supplier Fraud)

**Low-$, high-Risk Reqs**
- HIPAA (464 Reqs totaling $359k – some lack BAA)
- IT/Cloud (305 Reqs totaling $353k)
- Open Source (73 Reqs totaling $65k)

**PO Leakage (per annum)**
- T&E (~$3.5M PO spend)
- P-card (~$3.5M PO spend)
- Supplier Fraud (~$600k to $10M)
- Invoices (Non-PO, After the Fact ~$100M)
- Invoices (Dups ~$150k)
Requisitions – Key Word, < $5k Count (compliance rules)

HIPAA:
- Diagnosis
- Patient, patient data/information
- Transcription/transcribe
- Health information
- 464 Reqs, $359k

InfoSec:
- AWS
- Development
- Data processing, store
- Hosting
- 305 Reqs, $353k

Open Source:
- Application development
- Web Design
- AGPL
- Coding
- 73 Reqs, $65k

Risky Expense Types:
- Software/license
- Pharma
- High-Risk Expense types
- Professional Svcs/Consult
- SaaS
- 494 Reqs, $938k

Potential for incurring legal costs, regulatory action & reputation damage if sensitive information is leaked through partners or data-sharing portals.
Pcard – Cloud Software purchases (~$12k, 131 tx)

Adobe Creative Cloud - $8k, 61 tx

Amazon Web Services - $2k, 17 tx

Dropbox - $500, 20 tx

GISCloud, GETCloud - $1,170, 33 tx

Potential for incurring legal costs, regulatory action & reputation damage if sensitive information is leaked through partners or data-sharing portals.
Presenters:
Jim Hine, Associate Vice Chancellor & Chief Procurement Officer, UC San Francisco
Jim.Hine@ucsf.edu

Vanessa Wong, Executive Director of Procurement & Supply Chain Solutions, UC San Francisco
Vanessa.Wong@ucsf.edu

Ted Walter, Senior Director, Product Management, FICO
TedWalter@fico.com